CYBERDIPLOMACY CHINA TERHADAP AMERIKA SERIKAT TAHUN 2013-2017

SKRIPSI

Untuk Memehui Persyaratan Memperoleh Gelar Sarjana Program Studi Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik

Oleh

Shafira Rizki Aulia

NIM. 145120400111048

PROGRAM STUDI HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS BRAWIJAYA

2018

LEMBAR PERSETUJUAN

***CYBERDIPLOMACY* CHINA TERHADAP AMERIKA SERIKAT TAHUN 2013-2017**

SKRIPSI

Disusun Oleh :

Shafira Rizki Aulia

145120400111048

Telah disetujui oleh dosen pembimbing :

Pembimbing Utama	Pembimbing Pendamping
Primadiana Yunita S.IP., MA	**Joko Purnomo, S.IP, MA**
NIK. 2016079006202001	**NIP.197804012009121002**

Mengetahui,

Ketua Program Studi Hubungan Internasional

Aswin Arryanto Aziz, S.IP., M.DevSt

NIP.197802202011121001

LEMBAR PENGESAHAN

***CYBERDIPLOMACY* CHINA TERHADAP AMERIKA SERIKAT TAHUN 2013-2017**

SKRIPSI

Disusun Oleh :

Shafira Rizki Aulia

145120400111048

Telah Diuji dan Dinyatakan LULUS dalam Ujian Sarjana pada Tanggal 11 Desember 2018

Tim Penguji:

Ketua Majelis Penguji

Dian Mutmainah, S.IP., MA
NIP : 197803192005012002

Sekretaris Majelis Penguji

Irza Khurun'in, S.IP., MA
NIK : 2017109105132000

Anggota Majelis Penguji 1

Primadiana Yunita S.IP., MA
NIK. 2016079006202001

Anggota Majelis Penguji 2

Joko Purnomo, S.IP, MA
NIP.197804012009121002

Mengetahui,

Dekan Fakultas Ilmu Sosial dan Ilmu Politik

Universitas Brawijaya

Prof. Dr. Unti Ludigdo, S.E., M.Si., Ak
NIP. 196908141994021001

LEMBAR PERNYATAAN ORISINILITAS

Yang bertanda tangan dibawah ini, saya Shafira Rizki Aulia dengan NIM 145120400111048 menyatakan dengan sesungguhnya bahwa skripsi berjudul "***Cyberdiplomacy* China terhadap Amerika Serikat Tahun 2013-2017**" adalah benar-benar karya saya sendiri. Hal-hal yang bukan karya saya dalam skripsi tersebut, telah diberi catatan kaki dan ditunjukan dalam daftar pustaka. Apabila dikemudian hari terbukti pernyataan saya tidak benar, maka saya bersedia menerima sanksi akademik berupa pencabutan skripsi dan gelar yang saya peroleh dari skripsi tersebut.

Malang, 2018

Yang Membuat Pernyataan

Shafira Rizki Aulia

NIM. 145120400111048

KATA PENGANTAR

Alhamdulillah, Puji dan syukur kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah, serta karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "***CYBERDIPLOMACY* CHINA TERHADAP AMERIKA SERIKAT TAHUN 2013-2017"** sebagai salah satu syarat yang harus ditempuh untuk menyelesaikan Pendidikan Strata 1 (S1) pada Program Studi Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Brawijaya.

Penulis menyadari bahwa skripsi ini tidak akan terwujud tanpa adanya bantuan dan dorongan dari berbagai pihak. Oleh karena itu, penulis ingin mengucakan banyak terima kasih kepada:

1. Kepada Allah SWT yang telah memberikan karunia dan rahmatnya, sehingga penulis dapat meyelesaikan skripsi dengan sangat baik.
2. Ayahanda dan Ibunda tercinta, dan seluruh keluarga besar yang telah memberikan doa, dukungan materi dan non materi serta saran yang sangat membangun bagi penulis.
3 Pak Aswin Ariyanto Azis, S.IP., M. DevSt. Selaku ketua Program Studi Hubungan Internasional FISIP Universitas Brawijaya.
4. Dosen Pembimbing skripsi Ibu Primadiana Yunita, S. IP, MA., dan Bapak Joko Purnomo S. IP, MA.
5. Adik-adikku yang ngeselin tapi tetap memberikan *moral support* kepada penulis, Katlea Rizki Nabilah dan Adhitya Ferdiansyah.

6. Teman-teman Kos Bunga Andong, yaitu Kak Rury, Sarah, dan Selvi yang selalu ngingetin buat makan dan nanya udah makan belom karna mau deliv bareng. Yang selalu sabar menghadapi penulis dalam menyelesaikan skripsi ini, dan segala dinamika yang ada di kosan. memberikan kritik dan saran yang membangun kepada penulis, dalam keseharian maupun ketika dalam proses menyelesaikan skripsi ini.

7. Teman-teman SquadTenaga yang selalu melawak dan sangat menghibur penulis. Terima kasih ya gais semoga selalu berkembang untuk ga wacana mulu. *Keep it up ya guys*, pengalaman bareng kalian ga biasa emang LOL. Terima kasih telah memberikan informasi yang sangat informatif dari seputar gosip, dakwah, buka bersama, dan segala ajakan yang dadakan bagaikan tahu bulat, Marisya Anugrah, Gianinna Deva, Marutti Andriana, Chintia Dewi, Sabrina Inayati, Theresia Zabrina, Aulia Dwi Paras, dan Dea Pamungkas.

8. Terima kasih kepada teman seperjuangan seperbimbingan dan seperkomprean, Hapy Nabila. Inget Hap, *"hidup tiada mungkin… tanpa perjuangan, tanpa pengorbanan, mulia adanya". Terima kasih udah berjuang bareng!*. Jangan lupa, nanti kita sambat tentang hari ini.

9. Kolega Young On Top Malang yang sudah penulis anggap seperti keluarga sendiri karena ketemunya kalian lagi kalian terus sampe bosen .

10. Yonanda Dea Cahyono, Bella Claudia Amanda, Tika Madjid, yang menjadi dorongan penulis untuk terus ke perpustakaan pusat tanpa ada hasil yang signifikan, dan malah mengadakan forum gibah discussion dipimpin oleh mbak Yoyo. Sampai ketemu lagi ya chingu! <3.

11. Para K-squad sekalian : Adelia Dwi Wijayanti, Adela Rey Auladi dan Sita Mustika. Nomu gomawo chingu saranghaeyo~ noraebang kaja!.

12. Terima kasih kepada teman-teman H5 Chessy Oliviani, Diogo Bagaskara, Wulan Handayani dan Prasetyo Pangestu. Semoga tetap ambis dan produktif. See you when I don't want to see you.

13. Para manusia GARADA, yang meskipun jauh di mata tapi tetap di hati. Adlina Maharani, Andini Nursetiani, Dito Ilmam, Gita Larasati dan Muhammad Riza.

14. Terima kasih kepada serial tv Mr. Robot dan tokohnya yaitu Elliot Alderson dan Whiterose yang telah memberikan isnpirasi bagi penulis untuk menulis tentang *cybersecurity* dan hubungannya antara China dan AS yang pada akhirnya membuat penulis susah sendiri.

Penulis menyadari masih banyak kekurangan dan ketidaksempurnaan dari skripsi ini. Tetapi penulis sangat berterima kasih kepada seluruh pihak yang telah membantu penulis dalam proses pembuatan skripsi ini namun belum penulis sebutkan. Semoga skripsi ini bermanfaat bagi yang membaca.

Malang, Desember 2018

Penulis

ABSTRAK

Shafira Rizki Aulia (145120400111048). *Cyberdiplomacy* China terhadap Amerika Serikat tahun 2013-2017.

Perkembangan teknologi membawa perubahan dinamis dalam hubungan internasional. *Cyberspace* menjadi tantangan baru dalam bentuk persoalan keamanan non-tradisional maupun sebagai bentuk kekuatan negara. Hal tersebut menyebabkan timbulnya persaingan dalam *cyberspace* antar negara, dimana setiap negara berlomba untuk meningkatkan *cybersecurity* melalui kebijakan luar negeri. Salah satu cara untuk mencapai objektif negara dalam strategi *cybersecurity* internasional adalah melalui *cyberdiplomacy*. Dalam kasus negara China, *cybersecurity* merupakan persoalan keamanan nasional. China berupaya untuk meningkatkan kerjasama internasional *cybersecurity.* Meskipun memiliki rasa saling tidak percaya yang tinggi antara satu sama lain, China melakukan *cyberdiplomacy* terhadap AS dan berhasil mencapai kerjasama *cybersecurity* China-AS pada tahun 2015.

Kata Kunci : China, Amerika Serikat, Cyberdiplomacy, Cybersecurity.

ABSTRACT

Shafira Rizki Aulia (145120400111048). China's Cyberdiplomacy towards United States of America on 2013-2017.

The advancement of technology has created a dynamic shift in international relations. Cyberspace has brought new challenges, and become the new form of state power. For those reasons, *cyberspace* then become an arena of political contestation between states, in which every state is competing to increase their *cybersecurity* by means of foreign policy. One way to pursue the objectives of international cybersecurity strategies is to get through cyberdiplomacy. In the case of China, cybersecurity is all about national security. China is trying to enhance international cybersecurity cooperation. Although there are differences in the values of cyberspace and strategic distrust, China is conducting cyberdiplomacy towards United States and finally made a cybersecurity agreement in 2015.

Keywords: China, United States of America, Cyberdiplomacy, Cybersecurity.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GRAFIK

DAFTAR ISTILAH

CCP : *Chinese Communist Party*

OCCSIC : *Office of the Central Cyber Security and Informatization Commission*

CCCPC : *Central Committee of the Communist Party of China*.

PLA : *The People's Liberation Army*

TIK : Teknologi Informasi dan Komunikasi

KLN : Kementerian Luar Negeri

CICIR : *China Institute of Contemporary International Relations*

CSIS : *Center for Strategic and International Studies*

CGI : *Cybersecurity Global Index*

CAC : *The Cyberspace Administration of China*

ISILSG : *the Internet Security and Informatisation Leading Small Group*

EMCE : *Economic Motive Cyber Espionage*

S&ED : *U.S.-China Strategic and Economic Dialogue*

CWG : *U.S.-China Cyber Working Group*

LECD : *U.S.-China Law Enforcement and Cybersecurity Dialogue*

UN GGE : *United Nations Group of Governmental Experts*

NATO : *The North Atlantic Treaty Organization*

CERT : *Computer Emergency Response Team*

NSA : *National Security Agency*

WIC : *World Internet Conference*

BEC : *Business Email Compromise*

SCO : *Shanghai Cooperation Organisation*

GCCS : *Global Conference on Cyberspace*

CBM : *Confidence Building Measure*

MLAA : *Mutual Legal Assistance Agreement*

LOAC : *Laws of Armed Conflict*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi dan informasi memunculkan ranah baru dalam keamanan suatu negara. Permasalahan keamanan tidak lagi hanya persoalan keamanan fisik, tetapi juga non-fisik seperti yang terjadi dalam ranah *cyber*. Pada saat ini, penggunaan teknologi dan internet lekat dengan kehidupan setiap individu, dan setiap perangkat saling terhubung satu sama lain. Hal ini tergambar dalam konsep yang dinamakan *'Internet of Things'*.[1] Negara sebagai entitas tertinggi harus menghadapi perkembangan teknologi yang sangat pesat. *Cyberspace*[2] kemudian menjadi salah satu domain **s**trategis dalam pertahanan dan keamanan sebuah negara.[3] Berbagai aktor selain aktor negara seperti pemerintah negara lainnya, maupun aktor non-negara yang terorganisasi seperti organisasi kriminal dan kelompok teroris, hingga aktor non-negara yang tidak terorganisasi dapat menimbulkan ancaman dalam *cyberspace.*

[1] Mohamed Abomhara and Geir M. Køien, 'Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,' *Journal of Cyber Security* vol. 4 (2015), pp. 65–88 (p. 65).

[2] ***Cyberspace*** dilihat dalam isitlah teknologi adalah sebuah ruang *cyber* atau dunia virtual baik meliputi aktivitas yang dihubungkan oleh jaringan internet melainkan juga infrastruktur fisik yaitu komputer dan teknologi fisik lainnya. Pemahaman *cyberspace* dalam ilmu sosial tidak hanya sebatas produk teknologi dan jaringan internet, tetapi juga berhubungan dengan struktur sosial kehidupan masyarakat. Bersumber dari Anthimos Alexandros Tsirigotis, *Cybernetics, Warfare and Discourse: The Cybernetisation of Warfare in Britain*, (Springer, 2017), p. 46-47.

[3] Ibid., p. 20.

Dalam keilmuan hubungan internasional, isu *cybersecurity*[4] mulai menjadi sorotan sebagai isu keamanan non-tradisional. Isu keamanan tidak lagi hanya berada pada keamanan tradisional seperti peperangan maupun penggunaan senjata nuklir.[5] Setiap negara berupaya meningkatkan strategi keamanan nasional di bidang *cybersecurity*. Pada saat ini, sebanyak 82 negara di dunia telah memiliki strategi *cybersecurity* nasional.[6] Kesadaran akan ancaman dalam *cyberspace* memunculkan alat negosiasi dan perjanjian sebagai pendekatan baru untuk menghadapi permasalahan *cybersecurity* secara internasional. Diskusi internasional dalam isu *cybersecurity* mulai berfokus pada pembentukan norma dan nilai dalam tata kelola internet dan pentingnya kerjasama antar negara.

Isu *cybersecurity* mulai menjadi perhatian PBB pada tahun 1998, pada saat Rusia pertama kalinya memberikan draf resolusi mengenai *cybersecurity*. *UN Group of Governmental Experts* (UN GGE) adalah pertemuan multilateral yang untuk pertama kalinya berhasil mengatur hukum yang berlaku dalam *cyberspace*.[7] 15 negara, termasuk China, Rusia dan AS sepakat bahwa setiap negara wajib

[4] ***Cybersecurity*** adalah kumpulan kebijakan dan aksi yang digunakan untuk melindungi jaringan yang saling terhubung (termasuk juga alat elektronik, komputer, perangkat keras, dan kumpulan informasi) dari akses ilegal, pencurian data, modifikasi, dan ancaman lainnya., dideskripsikan oleh ITU, *Overview of Cybersecurity. Recommendation ITU-T X.1205*, 2009, p. 7 <http://www.itu.int/rec/T-REC-X.1205-200804-I/en> [accessed 2 February 2018].

[5] Nir Kshetri, 'Cybercrime and cyber-security issues associated with China: some economic and institutional considerations', *Electronic Commerce Research* no. 13 (2013), pp. 41–69 (p.42).

[6] NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Security Strategy Documents*, <https://ccdcoe.org/cyber-security-strategy-documents.html> [accessed 7 April 2018].

[7] UN GGE adalah komite *cyberspace* yang berisi Dewan Keamanan PBB. Pada tahun 2010, keputusan akhir UN GGE mengatakan bahwa hukum internasional juga berlaku dalam *cyberspace*, terutama hukum yang berasal dari keputusan PBB. Adam Segal, 'Chinese Cyber Diplomacy in a New Era of Uncertainty', *Hoover Working Group on National security, Technology, and Law*, Aegis Paper Series No. 1703, (Stanford University, 2017), p. 6.

mematuhi hukum internasional dalam *cyberspace*[8], dan menghormati kedaulatan negara begitu juga dengan prinsip dan norma yang dianut satu sama lain.[9]

Pentingnya *cybersecurity* menjadi *wake-up call* bagi berbagai negara di dunia, salah satunya adalah China. China merupakan sebuah negara besar dengan jumlah penduduk sebanyak 1.4 Milyar penduduk.[10] Tak hanya itu, setengah dari populasi tersebut dapat membawa China sebagai negara dengan pengguna internet terbanyak di dunia dengan total pengguna sebanyak 772 juta penduduk.[11] Kedua angka tersebut cukup besar apabila dilihat sebagai potensi sumber daya manusia dalam ranah *cyberspace.*

Secara ekonomi, China adalah negara raksasa yang berada di posisi kedua perekonomian dunia. China memiliki karakteristik perekonomiannya sendiri yang menjadikannya sebagai kekuatan ekonomi. Selain memiliki kekuatan dari jumlah populasi, China memanfaatkan tingkat penggunaan internet yang tinggi sebagai alat pertumbuhan bagi bisnis dan perkembangan pasar. Melalui bagan di bawah ini, terlihat bahwa meningkatnya jumlah pengguna internet berkorelasi dengan meningkatnya pertumbuhan ekonomi China.

---

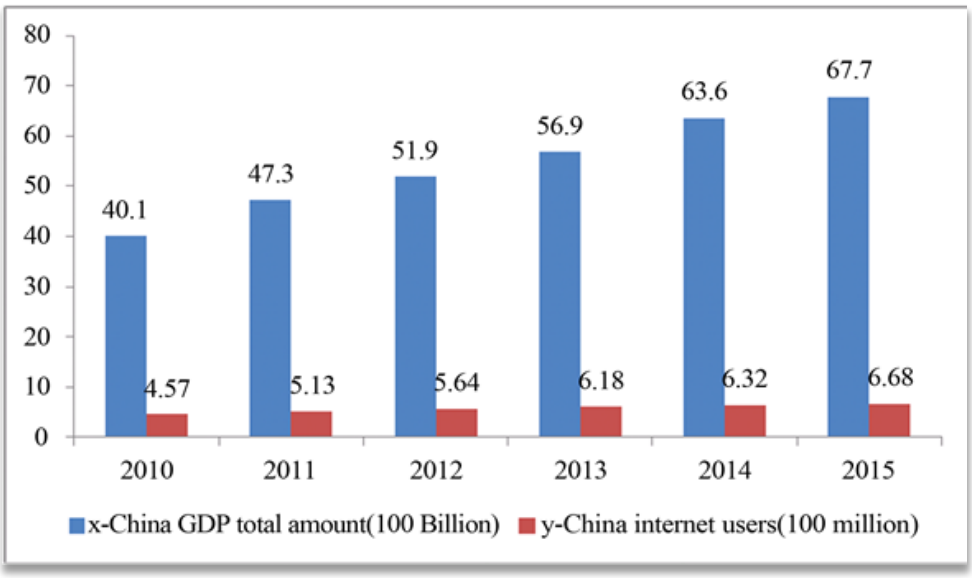
[8] General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *UN document A/65/201*, 2010, < http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf> [accessed 16 February 2018].

[9] General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *UN document A/68/98*, 2013, <www . un . org / ga / search / view _ doc . asp ? symbol= A / 68 / 98&referer= / english / &Lang = E> [accessed 5 July 2018].

[10]United Nations Department of Economic and Social Affairs, *Population And Vital Statistics Report Statistical Papers Series A Vol. LXX*, 2018, <https://unstats.un.org/unsd/demographic-social/products/vitstats/sets/Series_A_2018.pdf> [accessed 2 September 2018].

[11] China Internet Network Information Center (CNNIC), *Statistical Report on Internet Development in China*, 2018, p. 30 <https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf>[accessed 20 April 2018].

Grafik 1.1 Perbandingan Pertumbuhan Jumlah Total GDP dengan Pengguna Internet di Wilayah China



Sumber: Zhao, Z., Xiong, W. and Fang, J.X., 'Impact of Internet plus to China Economy Development'. *Modern Economy*, 7, (2016), p. 939.

Dewasa ini, perekonomian China sangat bergantung dengan teknologi informasi. *Cyberspace* memberikan nyawa dalam kemajuan sektor industri dan pengembangan ekonomi digital. Pada tahun 2017, pendapatan yang berasal dari perdagangan elektronik mengalami peningkatan sebanyak 43.4% per tahunnya, dengan total pendapatan 218.8 miliar RMB.[12] Angka tersebut menggambarkan bahwa *cybersecurity* kemudian berpengaruh terhadap keberlangsungan perekonomian China.

Tingginya tingkat pengguna internet dapat sekaligus menjadi potensi ancaman bagi stabilitas domestik, terlebih lagi bagi negara China yang merupakan negara dengan sistem satu partai. Ancaman tersebut dapat berasal dari pihak asing ataupun domestik. *Cyberspace* memiliki kapasitas sebagai sarana untuk melakukan

[12] China Internet Network Information Center (CNNIC), Loc.Cit., p. 12.

serangan yang ditujukan kepada pemerintah. Untuk mengantisipasi kerentanannya, pemerintah China lalu memberlakukan pengawasan terhadap aktivitas internet domestik, dan memperjuangkannya sebagai ranah kedaulatan teritorial secara internasional.[13]

Cybersecurity adalah prioritas keamanan nasional China pada rezim pemerintahan CCP saat ini.[14] Tidak hanya di bidang ekonomi, China mempersiapkan dirinya di era kemajuan teknologi di bidang keamanan melalui *cybersecurity*. Selaras dengan politik luar negerinya saat ini, China secara aktif berperan dalam pembentukan nilai dan norma *cyberspace,* terutama dalam hal tata kelola internet global. China memperjuangkan peran negara sebagai aktor utama yang berpengaruh dalam tata kelola internet global melaui *cyber sovereignty* atau kedaulatan internet, yaitu legitimasi atas kontrol dan manajemen konten internet yang ada di wilayahnya.[15]

Selain China, negara lainnya yang juga menganggap *cybersecurity* sebagai prioritas keamanan nasional dan bahkan mencoba untuk mendominasi ranah *cyberspace* adalah AS. Menempati posisi ke 2 dalam *Cybersecurity Global Index* (CGI), AS memiliki tingkat keamanan dan pertahanan *cybersecurity* yang dominan.[16] AS juga berperang aktif dalam tata kelola internet global. Tetapi, berbeda dengan China, AS menekankan peran yang dimiliki oleh *multi-stakeholder*,

---

[13] Greg Austin, C*ybersecurity in China The Next Wave*, (Springer, 2018), pp. 81-82.
[14] Xinhuanet, *The First Meeting of the Central Cyber Security and Informationization Leading Group Held an Important Speech by Xi Jinping*, 2014, <http://www.cac.gov.cn/2014-02/27/c_133148354.htm> [accessed 24 July 2018].
[15] Niels Nagelhus Schia and Lars Gjesvik, *China's cyber sovereignty*, The Norwegian Institute of International Affairs (2017), p. 1.
[16] International Telecommunication Union, *Global Cybersecurity Index 2017* <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf> [accessed 20 November 2017].

yaitu seluruh entitas yang menjadi stakeholder dalam *cyberspace* memiliki kewenangan yang sama dalam menentukan kebijakan tata kelola internet.[17] Hal tersebut selaras dengan nilai kebebasan internet, dan bagaimana AS menganggap ranah *cyber* sebagai sumber daya bersama atau *public goods.* Selain itu, sebagai negara pelopor perkembangan teknologi, AS memiliki posisi yang diperhitungkan dalam ICANN sebagai organisasi internasional yang mengontrol domain strategis *cyberspace.*

Pada tahun 2013, terjadi kasus "*prism gate",* yaitu pembeberan Edward Snowden mengenai aktivitas NSA yang melakukan pengawasan terhadap berbagai negara di dunia melalui *cyberspace* menggunakan 'pintu belakang' yang dibuat di dalam teknologi yang digunakan oleh masyarakat China.[18] China lalu menyadari ancaman terhadap ketergantungannya terhadap teknologi AS, dan bahaya yang ditimbulkan dari keterbukaan internet. Keamanan informasi masyarakat China bergantung pada sistem operasi yang dimiliki oleh beberapa perusahaan teknologi AS seperti halnya Microsoft.[19] Terlebih lagi, serangan *cyber* yang mengancam sistem informasi China dianggap paling banyak berasal dari AS.[20] Hal tersebut menimbulkan dilema bahwa penggunaan terhadap teknologi AS menyebabkan kerentanan terhadap keamanan informasi dalam ranah *cyber*, tetapi juga ancaman terhadap keluarnya data dan informasi China kepada AS.

---

[17] Zhang Xinbao, 'The Governance Model of Cyberspace Sovereignty and Its System Construction', *Chinese Social Sciences*, No. 8, 2016, p. 534.
[18] Lana Lam & Stephen Chen, 'US spies on Chinese mobile phone companies, steals SMS data: Edward Snowden', *South China Morning Post*, 2013, <https://www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden> [accessed 27 November 2017].
[19] Lu Chuanying, *The Power Game, Idea Evolution and China Strategy of Cyberspace Governance*, 2015, p. 121, & Austin, Loc.cit., p. 57.
[20] Lindsay, Min Cheung, & Reveron, Loc. Cit., p. 235.

Kasus Prism Gate membuktikan bahwa dengan membiarkan AS sebagai kekuatan tunggal *cyberspace,* beserta dengan pemikiran tata kelola internet *multi-stakeholder* hanya akan menciptakan celah ketidakamanan bagi negara yang rentan terhadap *cyber attack,* terutama negara-negara berkembang. China menekankan bahwa keamanan *cyber* hanya akan tercipta apabila seluruh negara di dunia berpartisipasi dalam tata kelola internet. Untuk itu, China tidak dapat membiarkan internet tanpa adanya pengawasan negara, dan menekankan pada peran negara sebagai penjaga keamanan dari *cybersecurity*. China kemudian mendorong tata kelola internet yang bersifat multilateral melalui *cyber sovereignty.*[21]

Strategi *cybersecurity* China lalu berfokus pada penguatan *cyber* yang dilakukan dalam bentuk peningkatan pengembangan teknologi, peningkatan keamanan internet, dan penguatan posisi China dalam tata kelola internet global. Presiden Xi Jinping kemudian berambisi menjadikan China sebagai *cyberpower*.[22] Salah satu strategi yang dilakukan oleh China adalah membawa *cyber sovereignty* dalam tata kelola internet global, yang mana hal itu dapat mendukung peran negara sebagai pemilik kewenangan tertinggi dalam *cyberspace.*

Mewujudkan *cyber sovereignty* membutuhkan kerjasama yang dilakukan oleh setiap negara. Di bawah kerangka *community of common destiny,* China berupaya untuk meningkatkan kerjasama internasional dalam bidang *cybersecurity,*

[21] Binxing Fang, *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace,* (Springer, 2018), pp. 122-123.
[22] Negara *cyberpower* adalah negara yang memiliki kemampuan menggunakan *cyberspace* untuk menciptakan keuntungan dan mempengaruhi peristiwa dalam lingkungan operasional lainnya dan antar berbagai instrumen *power*. Dikutip dari Daniel T. Kuehl, "From Cyberspace to *Cyberpower*: Defining the Problem," in Franklin D. Kramer, Stuart Starr, and Larry K. Wentz, eds., *Cyberpower* and National Security (Washington, D.C.: National Defense UP, 2009), p. 28.

termasuk juga dengan AS.[23] Tetapi, hubungan *cybersecurity* China-AS diwarnai rasa saling tidak percaya satu sama lain. Untuk mempertemukan pemikiran kedua belah pihak, China berpartisipasi dalam dialog bilateral yang dilakukan oleh perwakilan pemerintah bersama dengan pakar *cybersecurity* China maupun AS.

China dan AS lalu bertemu pada tahun 2013 untuk membahas perihal isu *cybersecurity*. Walaupun sempat menandakan sinyal positif, pada akhirnya pertemuan tersebut tidak membuahkan hasil yang signifikan. Tidak terlihat adanya perubahan perilaku keduanya yang masih saling tidak percaya terhadap satu sama lain. Forum dialog *cybersecurity* berakhir dengan pernyataan China yang memutuskan untuk menunda forum dialog bilateral China-AS dalam kurun waktu yang tidak dapat ditentukan.[24] Pada tanggal 24-25 September 2015, China dan AS melahirkan kesepakatan bilateral *'US-China Cyber Agreement 2015'* yang berbunyi:

> *"Both sides agree to step up crime cases, investigation assistance and information-sharing. And both government will not be engaged in or knowingly support online theft of intellectual properties."* [25]

Kutipan diatas mengatakan bahwa kedua belah pihak sepakat untuk menghentikan segala kegiatan spionase spionase siber dengan motif ekonomi, dan tidak terlibat maupun mendukung aktivitas pencurian kekayaan intelektual. Kesepakatan tersebut menandai dimulainya kerjasama antara AS dan China dalam menghadapi ancaman *cyber*.[26] Setelah tercapainya kerjasama *cybersecurity*,

[23] Ibid.
[24] Harold, Libicki, & Cevallos, Loc. Cit, p. 47.
[25] Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint> [accessed 2 December 2017].
[26] Harold, Libicki, & Cevallos, Loc cit, p. 9.

perjanjian yang telah disepakati pada tahun 2015 dilanjutkan dengan dialog tingkat tinggi dengan nama *U.S.-China Law Enforcement and Cybersecurity Dialogue* (LECD), sebuah kerangka kerjasama China-AS yang juga memasukkan unsur agenda kerjasama di bidang penegakan hukum.[27]

Dilihat dari sudut pandang *cyberdiplomacy*, tercapainya kesepakatan antara China dan AS adalah studi kasus yang menarik. Dibalik rasa tidak percaya satu sama lain, China dan AS berhasil mencapai kesepakatan melalui kerjasama *cybersecurity* China-AS tahun 2015.[28] Mengidentifikasi pelaku spionse *cyber* adalah perkara sulit, begitu juga dengan membangun kepercayaan dalam *cyberspace.* Terlebih lagi, China dan AS adalah dua negara dengan kepentingan yang saling bertolak belakang dalam tata kelola internet. AS adalah negara demokratis yang mendukung nilai kebebasan dalam berinternet, dan bertolak belakang dengan China yang berpegang teguh pada kedaulatan internet.[29] Untuk pertama kalinya, kesepakatan mengenai *cybersecurity* dengan isu utama spionase siber berhasil dicapai oleh China dan AS. Kerjasama *cybersecurity* China dan AS menjadi sebuah sinyal yang baik dalam perkembangan hubungan keduanya di ranah *cyber*.

---

[27]Department of Justice United States of America, *First U.S.-China Law Enforcement and Cybersecurity Dialogue Summary of Outcomes,* Available from: <https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue> [25 December 2017].

[28] Thomas Renard, *U S-China cybersecurity agreement: a good case of cyber diplomacy*, (2015), http://www.egmontinstitute.be/us-china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy/> [28 December 2017].

[29] Harold, Libicki, & Cevallos, Loc. Cit, p. 29.

1.2 Rumusan Masalah

Rumusan masalah yang dikaji dalam penelitian ini adalah "Bagaimana *cyberdiplomacy* China terhadap Amerika Serikat tahun 2013-2017?".

1.3 Tujuan Penelitian

Mengetahui *cyberdiplomacy* China terhadap Amerika Serikat tahun 2013-2017.

1.4 Manfaat Penelitian

Manfaat akademis penelitian:

1. Memberikan pengetahuan mengenai *cyberdiplomacy* China dalam domain strategis *cybersecurity*.
2. Memberikan kontribusi bagi perkembangan literatur terkait *cyberdiplomacy* China dan hubungannya dengan AS dalam domain *cyber*.

Manfaat praktis penelitian:

1. Manfaat penelitian ini adalah untuk memberikan kontribusi dalam kajian studi hubungan internasional.
2. Memberikan sumbangsih bagi penelitian lanjutan terkait *cyberdiplomacy* China dan hubungannya dengan AS dalam domain *cyber*.

BAB II

KAJIAN PUSTAKA

2.1 Studi Terdahulu

Studi terdahulu digunakan dalam penulisan untuk menganalisa poin pertanyaan penelitian. Untuk penelitian ini penulis akan menggunakan dua studi terdahulu berupa thesis. Studi terdahulu dipilih berdasarkan persamaan isu pembahasan dan penggunaan alat analisa yang sesuai dengan fokus pembahasan.

Studi terdahulu pertama merupakan sebuah thesis yang ditulis oleh Gabriele Pierini berjudul "*Cyber Security Meets Diplomacy: The EU-NATO Cooperation And The Italian Case*" yang ditulis pada tahun 2017. Penelitian ini adalah penelitian mengenai kerjasama *cybersecurity* yang dilakukan oleh UE dan NATO dengan fokus pembahasan pada *cyberdiplomacy* secara multilateral. Penulis menjelaskan *cyberdiplomacy* yang dilakukan secara multilateral oleh kedua aktor yaitu UE dan NATO. Keduanya memiliki objektif, instrumen dan struktur organisasinya masing-masing, tetapi keduanya digunakan negara Eropa untuk meningkatkan keamanan *cybersecurity*. Di akhir penulisannya, Pierini menjelaskan peran negara Italia dalam mendorong keberhasilan *cyberdiplomacy* kedua institusi tersebut.

Sebelum berfokus pada *cyberdiplomacy*, Pierini menjelaskan mengenai perkembangan diplomasi saat ini dengan menyorot pada pentingnya *cyberspace* sebagai ranah baru untuk mencapai tujuan suatu negara. *Cyberspace* merupakan dampak perkembangan teknologi yang memberikan ancaman baru bagi negara. Ancaman tersebut tidak hanya berasal dari aktor negara bahkan dari aktor non

negara sekalipun. Untuk itu, negara membutuhkan kerjasama satu sama lain meskipun dengan kepentingannya masing-masing.[30]

Pierini menjelaskan *cyberdiplomacy* menggunakan pendekatan pada *cybersecurity* UE dan NATO terlebih dahulu. Pierini menjelaskan perkembangan strategi *cybersecurity* berdasarkan objektif, konteks hukum, agensi dan kebijakan, dan juga pendanaan.[31] Lalu, kerjasama yang disepakati UE dan NATO ditekankan Pierini sebagai keberhasilan *cyberdiplomacy* dengan cara saling bahu-membahu dalam mengatasi permasalahan dalam *cybersecurity* bagi negara-negara Eropa. Kerjasama UE-NATO berawal pada tahun 2010 melalui berbagai pertemuan informal dan konsultasi tingkat tinggi. Lalu, NATO membentuk sebuah *liaison* dengan Agensi Pertahanan UE yang bertugas sebagai wadah pertukaran informasi. Pada tahun 2016, kedua belah pihak menandatangani perjanjian yang lebih bersifat teknis mengenai prosedur untuk mencegah, mendeteksi dan merespon kejadian *cyber*. Kerjasama tersebut kemudian berproses hingga menjadi proposal implementasi kebijakan *NATO-EU Joint Declaration 2016* yang menekankan pada penanganan ancaman *cyber*security, kemampuan pertahanan, penelitian R&D dan juga koordinasi dalam implementasinya.[32]

Pierini menjelaskan peran Italia sebagai pendukung utama dalam upaya dua organisasi tersebut utuk meningkatkan keamanan dan stabilitas regional melalui manajemen krisis. Italia memiliki perkembangan strategi *cybersecurity* yang baik, sehingga Italia dapat memberikan gambaran luas dalam diplomasi multilateralnya

[30] Gabriele Pierini, 'Cyber Security Meets Diplomacy: The EU-NATO Cooperation And The Italian Case' (International University for Social Studies "Guido Carli", 2017), p. 29.
[31] Ibid., p. 31.
[32] Ibid., pp. 66-68.

dalam negosiasi kerjasama *cybersecurity* UE-NATO.[33] UE dan NATO memiliki kemampuannya masing-masing, dan kerjasama yang disepakati dapat menjadikan kedua institusi tersebut memiliki pertahanan dan intelijensi yang lebih baik.

Temuan dalam penelitian ini adalah kerjasama *cybersecurity* UE-NATO dibutuhkan oleh kedua belah pihak. *Cyberdiplomacy* sangat erat kaitannya dengan tujuan, nilai, dan arah kebijakan masing-masing institusi. Dalam kerjasama multilateral, nilai yang dianut dan kepentingan dalam sebuah isu menentukan seberapa penting isu tersebut. Bagi NATO, isu *cybersecurity* merupakan permasalahan keamanan nasional yang cukup genting dan membutuhkan sistem pertahanan yang lebih dari pertahanan biasa. Tetapi di sisi lain, Pierini meragukan bahwa kerjasama yang dilakukan masih belum cukup untuk mengatasi tantangan dalam *cyberspace*.[34] Selain kerjasama, dibutuhkan koordinasi yang dapat menyatukan UE dan NATO agar tidak terjadi tumpang tindih kebijakan. Pierini berpendapat bahwa meskipun belum terlihat adanya keselarasan, kabar baiknya adalah kedua belah pihak sama-sama telah menuju pada satu tujuan yang sama yaitu *cybersecurity* terhadap ancaman *cyberspace*, dan menggunakan spesialisasinya di bidang keamanan untuk mencapai tujuan bersama tersebut.[35]

Persamaan penelitian Pierini dengan penelitian penulis adalah sama-sama menggunakan konsep *cyberdiplomacy,* sedangkan perbedaannya terletak pada studi kasus yang diambil. Penelitian Pierini melihat *cyberdiplomacy* yang dilakukan oleh UE dan NATO dalam mencapai kerjasama *cybersecurity*, sedangkan penulis

[33] Ibid., p. 77.
[34] Ibid., pp. 108-109.
[35] Ibid.

mencoba melihat *cyberdiplomacy* dalam kerjasama *cybersecurity* China-AS. Penulis melihat bahwa aktor *cyberdiplomacy* Pierini adalah banyak negara, sehingga *cyberdiplomacy* dilakukan secara multilateral. Sedangkan penelitian penulis menggunakan diplomasi bilateral. Selain itu, kedua aktor tersebut apabila dilihat dalam sudut pandang lebih luas memiliki pandangan tata kelola internet yang sama yaitu kebebasan informasi dalam berinternet. Berbeda dengan aktor yang diteliti oleh penulis dimana China dan AS memiliki pandangan tata kelola internet yang berbeda.

Kontribusi yang diberikan oleh penelitian Pierini terhadap penelitian penulis adalah penulis menemukan bahwa *cyberdiplomacy* dapat dijelaskan melalui startegi *cybersecurity* suatu negara yang kemudian dihubungkan dengan Strategi diplomasi. Selain itu, penulis dapat mengetahui pentingnya tujuan dan kepentingan yang dimiliki oleh setiap aktor dalam menentukan tercapainya suatu kerjasama, terutama apabila aktor yang digunakan memiliki sudut pandang akan isu *cybersecurity* yang berbeda. *Cyberdiplomacy* pada akhirnya menjadi jalan yang diambil untuk menghadapi tantangan dalam *cyberspace.*

Studi terdahulu kedua adalah thesis yang ditulis oleh Joseph B. M. Chua berjudul **"***2015 U.S.–CHINA CYBER AGREEMENT: A NEW HOPE, OR "THE EMPIRE STRIKES BACK"?"*, dan ditulis pada tahun 2017. Dalam penelitiannya ini, Chua menjelaskan efektivitas kerjasama *cyberecurity* yang dilakukan oleh China dan AS tahun 2015, dan implikasi perjanjian tersebut pada hubungan China-AS kedepannya.

Pada tahun 2015 China dan AS mencapai kesepakatan perihal kerjasama dalam *cybersecurity*. Padahal, sebelumnya terdapat ketidakpercayaan yang kuat terhadap satu sama lain dan saling tuduh menuduh terkait aktivitas spionase siber. AS menganggap China sebagai pelaku spionase siber yang didukung oleh hasil penelitian lembaga *cybersecurity* Mandiant yang berjudul *"APT1: Exposing One of China's Cyber Espionage Units"*. Sedangkan di sisi lain, China juga menganggap AS sebagai ancaman spionase siber terutama setelah terkuaknya dokumen NSA milik Edward Snowden. Tetapi kerjasama antara keduanya berhasil dicapai. Chua berargumen bahwa kerjasama ini merupakan kerjasama yang membawa sinyal positif dalam perkembangan hubungan China AS dalam ranah *cyber*.

Efektivitas dari kerjasama tersebut diukur melalui beberapa analisis. Pertama adalah melalui analisis kerugian sebagai dampak *cybersecurity*. Dengan adanya kerjasama, maka kedua belah pihak dapat mengurangi kemungkinan akan kerugian yang muncul dari ancaman *cyberspace*. Kedua, dengan adanya perjanjian tersebut, muncul kebijakan-kebijakan yang dikeluarkan untuk mengatasi *cybercrime*.[36] Kesadaran akan ancaman *cyberspace* telah ada dalam sudut pandang keamanan nasional, yang kemudian diimplementasikan melalui kebijakan nasional. Selain itu, kerjasama spionase siber juga berdampak pada tata kelola internet global. Dengan adanya kerjasama mengenai spionase siber, China dan AS berhasil mengirimkan pesan kepada masyarakat global mengenai norma perilaku dalam

[36] ***Cybercrime*** adalah aktivitas ilegal yang dilakukan dalam *cyberspace*, dan memberikan ancaman pada keamanan nasional suatu negara. Aktivitas tersebut antara lain adalah akses ilegal terhadap komputer milik orang lain, dan membuat, menyebarkan, dan menggunakan perangkat lunak sebagai alat untuk mengganggu sistem operasi pada komputer. Setiap negara memiliki definisi berbeda-beda terhadap aktivitas ilegal yang termasuk dalam *cybercrime*. Bersumber pada Klimburg, Op.Cit., p. 13-15.

cyberspace. Aktivitas spionase untuk mengambil keuntungan merupakan aktivitas ilegal, tetapi tidak dijelaskan secara lebih lanjut untuk kasus spionase dengan kepentingan politik.[37] Dengan kata lain, kerjasama tersebut membawa dampak pada tata kelola internet global, meskipun tidak dilakukan dalam forum multilateral.

Chua mengemukakan bahwa terdapat perbedaan kebijakan yang diambil oleh China berdasarkan kurun waktu yang dibedakan menjadi sebelum hingga sesudah kerjasama. Sebelum adanya perjanjian tersebut, kebijakan China terhadap *cybersecurity* masih sangat minim. Tetapi setelah adanya perjanjian, China mulai menunjukkan perhatian lebih terhadap *cybersecurity* dalam kebijakan domestik maupun kebijakan luar negerinya.[38] Salah satunya adalah dibentuknya *cybersecurity law*, hukum yang mengatur keamanan data bagi semua perusahaan yang ada di China. Setelah adanya perjanjian pun terlihat bahwa terjadi pengurangan aktivitas spionase siber yang dilakukan oleh China terhadap AS.[39] Melalui kebijakan yang diambil dalam aspek domestik dan internasional, Chua berpendapat bahwa terlihat adanya upaya China untuk mematuhi kerjasamanya dengan AS dalam bidang *cybersecurity.*

Persamaan penelitian yang dilakukan penulis dengan penelitian milik Joseph B. M. Chua terletak pada subjek penelitian yaitu kerjasama *cybersecurity* China-AS pada tahun 2015. Perbedaannya adalah penelitian milik Chua tidak berfokus pada *cyberdiplomacy* yang dilakukan oleh China dan AS, melainkan efektivitas dari kerjasama tersebut dan memprediksikan implikasinya. Meskipun

[37] Joseph B. M. Chua, '2015 U.S.-China *Cyber* Agreement: a new hope, or "the empire strikes back"?' (Monterey, California: Naval Postgraduate School, 2017), p. 28.
[38] Ibid., p. 35.
[39] ibid., pp. 23-27.

memiliki perbedaan fokus penelitian, tetapi, seperti yang telah dijelaskan sebelumnya, subjek penelitian penulis dan penelitian Chua memiliki kesamaan. Sehingga penelitian yang dilakukan Chua dapat menjadi argumen pendukung bagi penelitian penulis.

Sedangkan kontribusi penelitian bagi penelitian penulis adalah dengan menggunakan penelitian Chua sebagai studi terdahulu penulis dapat mengetahui gambaran secara menyeluruh mengenai kerjasama *cybersecurity* China-AS pada tahun 2015 beserta analisis-analisisnya. Analisis Chua berpusat pada posisi China sebelum tercapai kesepakatan hingga setelah melakukan kesepakatan dengan AS, dan bagaimana efektivitas kerjasama tersebut dalam hubungan China dan AS dalam isu *cybersecurity.*

2.2 Kerangka Konseptual

2.2.1 Konsep Diplomasi

Kolaborasi internasional melalui sebuah kerjasama adalah salah satu cara yang dapat digunakan pemerintah untuk mencapai tujuannya. Negara beraliansi maupun membentuk sebuah kerjasama berdasarkan kepentingan yang ingin dicapai kedua belah pihak. Kepentingan setiap pihak disampaikan melalui diplomasi. Diplomasi merupakan sebuah konsep yang digunakan untuk menjelaskan tindakan negara dalam mencapai tujuannya menggunakan sumber daya diplomatik. Konsep diplomasi mengandung unsur penting yaitu interaksi internasional dengan aktor lainnya, dan tujuan yang ingin dicapai dalam bentuk kepentingan nasional.

Perwakilan diplomatik membawa kepentingannya masing-masing dan berkomunikasi dengan satu sama lain melalui dialog formal maupun informal.[40]

Salah satu cara yang dilakukan dalam diplomasi adalah negosiasi. Representasi kepentingan nasional disampaikan melalui diskusi untuk mencapai kerjasama terkait isu yang diangkat oleh semua pihak.[41] Apabila sebuah kerjasama berhasil disepakati, maka tujuan dari kerjasama tersebut menjadi kepentingan yang diakomodasi oleh semua pihak. Tujuan dari diplomasi itu sendiri dapat berupa aliansi di bidang ekonomi maupun keamanan.[42]

Diplomasi terbagi menjadi diplomasi bilateral dan diplomasi multilateral. Diplomasi bilateral adalah suatu hubungan diplomatik yang dilakukan oleh dua negara, sedangkan multilateral adalah hubungan diplomatik yang dilakukan oleh lebih dari dua atau banyak negara. Ketika kerjasama telah tercapai, dilakukan proses tindak lanjut dari kerjasama tersebut. Dalam diplomasi bilateral, tindak lanjut yang dilakukan berupa pertemuan-pertemuan dan dialog bilateral untuk menegaskan kembali tujuan yang ingin dicapai dan cara implementasinya, juga langkah apa yang harus diambil selanjutnya. Sedangkan diplomasi multilateral menindak lanjuti kerjasama menggunakan konferensi internasional.[43]

2.2.2 *Cyberdiplomacy*

Perkembangan teknologi dan *cyberspace* menjadikan isu *cyber* semakin penting dalam ranah keamanan internasional. *Cyberspace* memunculkan adanya

[40] B. R. Gerridge, *Diplomacy: Theory and Practice* , Fourth Edition, (Palgrave : Hampshire : 2009), p. 1.
[41] Ibid., p. 25.
[42] Ibid., p. 28.
[43] Ibid., p. 94.

tantangan yang berupa peluang maupun ancaman bagi keamanan nasional. *Cyberspace* memberikan kemudahan bagi pemerintah untuk mengawasi warga negaranya. Tetapi, ancaman yang ditimbulkan *cyberspace* jauh lebih besar, terutama ancaman bagi infrastruktur fisik. Ancaman yang ditimbulkan dalam *cyberspace* antara lain adalah : terorisme, aktivitas kriminal, spionase, dan *cyberwar*[44], dimana aktivitas tersebut dapat dilakukan oleh aktor negara maupun non negara.[45] Proteksi kemudian diambil tidak hanya melalui sebatas *cybersecurity* tetapi juga mengintegrasikan *cyberspace* sebagai komponen dari kebijakan luar negeri.

Dalam bidang *cybersecurity,* diplomasi yang dilakukan disebut dengan *cyberdiplomacy*, sebuah konsep yang baru dalam hubungan internasional.[46] Penjelasan maupun definisi dari *cyberdiplomacy* itu sendiri masih berkembang hingga saat ini, begitu juga dengan mekanisme dalam *cyberdiplomacy.* Meskipun aktivitas diplomatik ini mulai beradaptasi dengan isu *cyber,* tetapi masih besar kesenjangan antara praktik dan penjelasan konseptual dalam *cyberdiplomacy.* Terminologi mengenai *cyberdiplomacy* masih belum disepakati secara universal, sehingga konseptualisasi dari *cyberdiplomacy* itu sendiri cukup sulit. Hal tersebut lalu berdampak pada isu *cyber* yang menjadi bagian dari *cyberdiplomacy.*

[44] ***Cyberwar*** adalah perang yang dilakukan dalam *cyberspace,* atau situasi konflik antar entitas politik, dimana para aktor menggunakan serangan *cyber* untuk mencapai tujuannya. Dikutip berdasarkan Elias G. Carayannis, David F.J. Campbell, & Marios P.E., *Cyber-Development, Cyber-Democracy and Cyber-Defense* (Springer, 2014), p. 262.
[45] Radu Constantin Mureșan, 'Current Approaches Of Diplomacy In The Cyberspace' (STUDIA UBB. EUROPAEA, LXII, 2, 2017), pp. 31-43, (p. 39).
[46] Ibid., p. 4.

Pada awalnya, konsep *cyberdiplomacy* digunakan untuk menjelaskan hubungan antara revolusi teknologi dan penggunaan internet sebagai alat diplomasi.[47] Akan tetapi, diplomasi yang dilakukan bersifat diplomasi publik[48], dan tidak memasukkan upaya diplomatik untuk menangani isu-isu yang mucul terkait *cyberspace* dalam aspek internasional. Literasi *cyberdiplomacy* kemudian berfokus pada pendekatan upaya diplomatik sebagai alat untuk mencapai kepentingan nasional dalam *cyberspace* dan menjadi bagian dari politik luar negri suatu negara. [49] Dengan begitu, *cyberdiplomacy* merupakan hasil dari politisasi isu *cyber* yang diimplementasikan melalui praktik diplomasi.

Cyberdiplomacy dijelaskan sebagai diplomasi yang dilakukan dalam domain *cyber* atau dengan kata lain menggunakan sumber daya diplomatik dan menjalankan fungsi diplomatik untuk mencapai kepentingan nasional dalam *cyberspace*.[50] Konsep *cyberdiplomacy* menjelaskan kegiatan diplomatik seperti dialog melalui wadah atau forum internasional, mekanisme identifikasi dan konsultasi multilateral, kesepakatan yang dicapai untuk mengurangi kesalahpahaman antar pihak, membentuk budaya global dalam ranah *cybersecurity*, identifikasi keuntungan yang ada dalam *cyberspace*, *confidence-building measure*[51]

---

[47] Potter, E. H., *Cyber-diplomacy: Managing foreign policy in the twenty-first century*, (Montreal: McGill-Queen's University Press, 2002), p. 3.

[48] *Public Diplomacy* atau diplomasi publik adalah instrumen yang digunakan pemerintah untuk membangun citra positif atas negaranya sendiri dengan tujuan untuk membangun opini. Dikutip berdasarkan Gerridge, Op.Cit., p. 179.

[49] André Barrinha & Thomas Renard, '*Cyber*-diplomacy: the making of an international society in the digital age', *Global Affairs*, (2017), pp. 1-12, (p. 4).

[50] Barrinha & Renard, Loc.cit., p 3.

[51] ***Confidence-building measure*** adalah tindakan yang mencerminkan iktikad dan kemauan untuk bertukar informasi dengan pihak lainnya. Tujuan dari *confidence-building* adalah untuk mengurangi keurigaan, ketakutan, kecemasan, dan konfil yang dialami oleh dua atau lebih pihak. Bersumber dari Sophie Harman, *Confidence-building measure*, <https://www.britannica.com/topic/confidence-building-measure> [accessed 3 May 2017].

antar negara, transparansi dalam komunikasi, atensi terhadap lemahnya *cybersecurity* internal, dan membangun kesadaran para pemangku kepentingan akan ancaman, resiko, dan celah dalam ranah *cyber*.[52]

Elemen dasar *cyberdiplomacy* adalah *cyber*, yang juga merupakan unsur utama konsep diplomasi lainnya yaitu *e-diplomacy*, atau *digital diplomacy*. Berbeda dari *e-diplomacy*, *cyberdiplomacy* tidak semata-mata adalah diplomasi menggunaan alat digital dan internet. *Cyberdiplomacy* menekankan pada aktivitas diplomatik dengan isu utamanya adalah *cybersecurity*. Hal tersebut menggambarkan adanya unsur kebijakan luar negeri yang diambil dalam sebuah agenda politik. *E-diplomacy* menekankan pada penggunaan alat digital dalam aktivitas diplomasi, dimana tujuan akhirnya tidak pasti mengenai isu dalam *cyberspace* itu sendiri. Untuk itu, distingsi antara *cyberdiplomacy* dan *e-diplomacy* terletak pada penggunaan alat digital oleh diplomat dan mentri luar negeri dengan diplomasi dalam *cyberspace*.[53]

Konsep *cyberdiplomacy* tidak terlepas dari upaya yang dilakukan negara untuk mencapai kepentingannya melalui hubungan dan interaksinya dengan negara lain. *Cyberdiplomacy* merupakan kegiatan diplomatik yang erat hubungannya dengan *cyberspace*, sehingga elemen dalam aktivitas diplomatik berkaitan erat dengan ranah *cyber* dan kebijakan luar negeri suatu negara. Berdasarkan penjelasan konsep *cyberdiplomacy* dapat diketahui variabel-variabel dalam pelaksanaan *cyberdiplomacy* itu sendiri yaitu *diplomatic activity*, *national interest*, *Strategic*

[52] Dana Danca, '*Cyber* Diplomacy — A New Component of Foreign Policy', *Journal of Law and Administrative Sciences*, Issue 3, (2015), pp. 93–97 (p. 93).
[53] Ibid.

issue, dan *diplomat*.[54] Setiap variabel berhubungan dengan *cyberspace*, dan juga kebijakan luar negeri. Penjelasan akan peranan setiap variabel adalah sebagai berikut:

2.2.2.1 *Diplomatic Activity*

Diplomat yang membawa kepentingan nasional berprakarsa melalui kegiatan diplomatik dengan membawa isu *cyber* internasional. Dalam menghadapi permasalahan *cyberspace,* diplomat seringkali dihadapkan dengan masalah penggunaan teknologi informasi dan komunikasi, *cybersecurity,* dialog *cyber* bilateral, pengembangan kebijakan, isu penggunaan internet, hak asasi manusia dalam era *cyber,* isu persoalan perdagangan dan hak kekayaan intelektual, dan isu-isu lainnya.[55] Tujuan dari diplomasi adalah meningkatkan kepercayaan satu sama lain dan menjaga stabilitas hubungan antar negara. Aktivitas diplomasi merupakan hal fundamental yang menjadi penopang eksistensi masyarakat internasional.

Berangkat dari pemahaman mengenai *cyberspace* sebagai ranah yang dapat diakses bebas oleh semua entitas, *cyberdiplomacy* menjadi hal yang dibutuhkan untuk mencapai kesepakatan dalam *cyberspace.* Sifat alami *cyberspace* diantaranya adalah bebas dan tidak terbatas. Identifikasi pelaku dalam *cyberspace* cukup sulit, dan negara tidak semata-mata dapat mencegah dan mengatur perilaku satu sama lain. Akibatnya, rasa saling tidak percaya terhadap satu sama lain sangat kental dalam ruang lingkup *cyberspace*, begitu juga dengan tata kelola *cyberspace* yang

[54] Barrinha & Renard, Loc.cit., pp 3-6.
[55] Heli Tiirmaa-Klaar, 'Cyber diplomacy: Agenda, challenges and mission', in K. Ziolkowski (Ed.), *Peacetime regime for state activities in cyberspace: International law, international relations and diplomacy* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), p. 509.

sulit untuk mencapai kesepakatan bersama. Di sisi lain, hal tersebut dimanfaatkan negara besar untuk kepentingannya masing-masing. Dengan demikian, untuk menghindari potensi konflik dalam *cyberspace*, perlu dicapai kesepakatan bersama melalui diplomasi. [56]

Dalam jurnalnya, Barrinha dan Renard menggunakan sudut pandang *english school* sebagai dasar dari *cyberdiplomacy*, yaitu adanya masyarakat internasional yang memiliki suatu tatanan dalam hubungannya satu sama lain.[57] *Cyberdiplomacy* kemudian dapat dilakukan dengan antar diplomat atau diplomat dengan aktor non-negara lainnya seperti pemimpin perusahaan internet, perusahaan teknologi, dan organisasi masyarakat. *Cyberdiplomacy* dilakukan melalui pertemuan dialog bilateral maupun multilateral. Dialog bilateral maupun multilareal merupakan langkah yang digunakan untuk menemukan titik temu dalam bernegosiasi dan menumbuhkan kepercayaan dalam isu *cyberspace*. Barrinha dan Renard menggambarkan dialog bilateral seperti halnya pertemuan yang dilakukan oleh China dan AS mengenai *cybersecurity*, sedangkan dialog multilateral seperti halnya forum UN GGE.[58]

2.2.2.2 *National Interest*

Setiap negara memiliki tujuan yang ingin dicapai melalui kebijakan luar negerinya yang disebut dengan *national interest* atau kepentingan nasional. Kepentingan nasional dalam *cyberspace* suatu negara direpresentasikan oleh diplomat melalui *cyberdiplomacy*. Kepentingan tersebut dapat diamati melalui

[56] Barrinha & Renard, Loc.cit. p. 5.
[57] Barrinha & Renard, Loc.cit., p. 2.
[58] Barrinha & Renard, Loc.cit., p. 3.

Strategi *cybersecurity* internasional, yang tidak hanya berisi mengenai Strategi keamanan tetapi juga prinsip dasar dan nilai dalam *cyberspace* suatu negara.[59] Melalui agenda itulah tersirat agenda diplomatik dalam kerangka diplomatik yang menjadi acuan pada saat membawa kepentingannya dalam aktivitas diplomasi.

Pada awalnya, isu *cyber* hanya sebatas pada permasalahan teknis terkait *cyberspace* dan juga keamanan domestik. Strategi *cybersecurity* seperti *White Paper on the internet in China,* hanya menekankan pada pentingnya peningkatan kapabilitas pertahanan dan keamanan infrastruktur jaringan internet.*[60]* Isu *cyber* kemudian dipolitisasi dan mengalami internasionalisasi, lalu menjadi bagian dari kebijakan luar negeri karena memiliki kepentingan *cyberspace* dalam hubungannya secara internasional. Terlihat dalam forum multilateral seperti UN GGE (*United Nations Group of Governmental Experts).* Tujuan forum multilateral tersebut adalah membangun norma tata kelola internet global, dimana setiap negara berupaya untuk memperjuangkan kepentingannya masing-masing.

2.2.2.3 *Cyber Issue*

Hubungan suatu negara memiliki gejolak konflik yang dapat disebabkan oleh ketidakpercayaan satu sama lain, atau komunikasi tidak sempurna. Konflik tersebut berada pada isu *cyber* tertentu, dimana setiap pihak berupaya mencapai penyelesaian masalah atas isu yang ada. Isu *cyber* yang diangkat merupakan aspek internasional dalam isu *cyber*.*[61]* Permasalahan mendasar dalam *cyberdiplomacy* adalah bagaimana negara menghadapi ancaman *cyber* menggunakan hukum

[59] Barrinha barrin& Renard, Loc.cit.
[60] Barrinha & Renard, Loc.cit., p. 6.
[61] Ibid.

internasional yang berlaku, maupun membangun norma perilaku dalam *cyberspace.*[62]

Isu *cyber* yang menjadi pokok pembahasan dalam aktivitas diplomatik baik sebatas isu *cyber* secara teknis maupun kebijakan domestik. Isu *cyber* tersebut dipolitisasi dan berada pada konteks kebijakan luar negri. Dalam melihat isu *cyber* yang menjadi tujuan kegiatan diplomatic dapat dilihat melalui *cyber agenda* yang dibawa dalam kegiatan diplomatik. Barrinha dan Renard menjelaskan bahwa *cyber issues* yang pada umumnya terdapat dalam agenda *cyberdiplomacy* diantaranya adalah *cybersecurity, cybercrime, confidence-building*, kebebasan berinternet dan tata kelola internet.[63] *Cyber agenda* tidak hanya terbatas pada satu isu. Dalam suatu pertemuan, beberapa agenda dapat menjadi topic diskusi atau mengenai suatu kerangka kerjasama secara keseluruhan.[64]

2.2.2.4 *Diplomat*

Aktor *cyberdiplomacy* adalah perwakilan resmi negara atau diplomat. Diplomat adalah perwakilan negara yang diutus untuk merepresentasikan kepentingan nasional melalui kegiatan diplomasi. Dalam *cyberdiplomacy*, peran diplomat menjadi penting, terutama perkembangan peran Kementerian Luar Negeri dalam menangani *cyber issues.* Diplomat yang melakukan *cyberdiplomacy* pada saat ini disebut sebagai ‘pionir’. Kebaruan konsep *cyberdiplomacy* menjadikan mereka sebagai generasi pertama yang mengimplementasikan konsep tersebut.[65]

[62] Danca, Loc.cit.
[63] Barrinha & Renard, Loc.cit.3
[64] Tiirmaa-Klaar, Loc. Cit., pp. 517-529.
[65] Barrinha & Renard, Loc.cit.

Perubahan dalam aktivitas diplomasi menuntut diplomat untuk dapat beradaptasi dengan isu yang selalu berkembang. *Cyberdiplomacy* tidak hanya membangun kolaborasi dan kerjasama internasional melalui diplomasi, tetapi juga berupaya untuk mengembangkan alat dan sistem teknologi yang dapat digunakan untuk meningkatkan *cybersecurity*.[66] Peran *cyberspace* yang semakin lama semakin signifikan bagi kepentingan nasional, menjadikan diplomat diharuskan untuk dapat menguasai penggunaan teknologi dan perkembangan istilah di dalamnya.

Ketika upaya *cybersecurity* hanya bersifat teknis dan tidak dilakukan oleh diplomat maka hal tersebut tidak dapat dikatakan sebagai *cyberdiplomacy*. Diplomat memiliki agenda diplomatik sebagai tanggung jawabnya. Diplomat membawa agenda mengenai isu *cyberspace* yang mengandung unsur politik sebagai bentuk kepentingan nasional. Berbeda halnya dengan upaya penanggulangan teknis mengenai isu *cyberspace* yang tidak melibatkan diplomat. Contohnya adalah CERT yaitu *Computer Emergency Response Team*, yang merupakan sekelompok tim ahli permasalahan keamanan komputer. Mereka berfokus pada penanganan teknis masalah dalam *cyberspace* meskipun dalam skala internasional, dan mereka tidak memiliki agenda diplomatik yang mengandung kepentingan politik didalamnya.[67]

Barrinha dan Renard menjelaskan bahwa dalam menangani isu *cybersecurity*, terdapat dua pendekatan institusional dalam melihat peran Kementerian Luar Negeri (KLN). Pertama adalah melakukan sentralisasi, yaitu

[66] Mureșan, Loc.cit, p. 40.
[67] Barrinha & Renard, Loc.cit.

membentuk sebuah departemen baru yang secara khusus menangani isu *cyber* di bawah KLN. Kedua, membentuk sebuah unit koordinasi baru yang berada di bawah KLN, dengan prinsip bahwa isu *cyber* merupakan isu yang bersinggungan dengan isu lainnya.[68]

2.3 Operasionalisasi Konsep

Penelitian penulis ini berupaya mengaitkan konsep *cyberdiplomacy* terhadap kerjasama *cybersecurity* China-AS tahun 2015 yang dilihat dari sudut pandang negara China. Penggunaan konsep *cyberdiplomacy* didasari dengan melihat kerjasama tersebut sebagai upaya China mencapai kepentingan nasionalnya melalui diplomasi bilateral dalam payung besar *cybersecurity*. Mengingat kegiatan diplomasi kini tidak hanya terintegrasi dengan teknologi secara teknis, tetapi juga telah menjadi aspek internasional dalam sudut pandang kebijakan luar negeri suatu negara.[69]

Konsep *cyberdiplomacy* memiliki beberapa variabel yaitu *cyber issue*, diplomat, kepentingan nasional, dan kegiatan diplomatik.[70] Kerjasama melalui *cyberdiplomacy* mengandung unsur interaksi antar negara dan penggunaan *cyber* untuk kepentingan dalam ranah *cyberspace.* Dalam penelitian ini penulis melihat *cyberdiplomacy* China melalui interaksi antara China dan AS dalam *cyberspace* pada kurun waktu 2013-2017.

[68] Barrinha & Renard, Loc.cit. pp. 7-8.
[69] Barrinha & Renard, Loc.cit.
[70] Barrinha & Renard, Loc.cit., pp. 3-6.

2.3.1 *Diplomatic Activity*

Kegiatan diplomatik dilakukan melalui sebuah wadah yang dapat memelihara hubungan *cybersecurity* kedua negara. Sebuah kegiatan diplomatik tentunya memiliki tujuan yang hendak dicapai. Penelitian ini menjelaskan kegiatan diplomatik yang dilakukan oleh China dan AS dalam isu *cybersecurity* sebagai upaya meningkatkan rasa percaya diantara kedua pihak. *Cyberdiplomacy* juga dilihat sebagai upaya China untuk mewujudkan tujuannya dalam hubungan China dengan negara lainnya dalam ranah *cybersecurity*.

China melakukan *cyberdiplomacy* dengan AS melalui dialog bilateral. Dialog tersebut dilihat sebagai upaya mewujudkan tujuan dari kerjasama yang diinginkan dan bentuk dari *cyberdiplomacy* China-AS. Penelitian ini menjelaskan dialog bilateral China dengan AS dalam ranah *cybersecurity* berdasarkan tujuan yang ingin dicapai China yaitu kerjasama internasional untuk membangun *"community of a common destiny",* salah satu politik luar negeri China. Karena, setiap *cyberdiplomacy* yang dilakukan secara bilateral maupun multilateral akan berkontribusi pada pembentukan unsur nilai dan norma perilaku dalam *cyberspace.*[71]

Penelitian ini akan melihat lima bentuk dialog yang dilakukan oleh China dan AS menuju kerjasama *cybersecurity* hingga telah menjadi sebuah mekanisme kerjasama.[72] Bentuk upaya tersebut antara lain; *US-China Cybersecurity Dialogue, U.S.-China Strategic and Economic Dialogue,* Kunjungan Kenegaraan Presiden Xi

[71] Klimburg, Op.cit., p. 99-100.
[72] Ziolkowski, 2013; Pawlak, 2015, Op.Cit.

Jinping ke Amerika Serikat, *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*, dan *U.S.-China Law Enforcement and Cybersecurity Dialogue*. Jalur diplomatik yang dilalui keduanya berada pada track 1.5 yang dinamakan dengan *US-China Cybersecurity Dialogue* dan dimulai sejak tahun 2009. Sedangkan diplomasi track 1 melalui *U.S.-China Strategic and Economic Dialogue* (S&ED) kelima. Didalamnya, isu *cybersecurity* menjadi agenda dalam perbincangan pertemuan kenegaraan kedua negara, dimana didalamnya dibentuk *U.S.-China Cyber Working Group* (CWG) sebagai satu kesatuan dalam rangkaian pertemuan tersebut. Penelitian ini tidak melihat S&ED lainnya, dikarenakan oleh CWG tidak mendapatkan kelanjutan dalam pertemuan S&ED selanjutnya.

Penelitian ini kemudian melihat kunjungan kenegaraan yang dilakukan presiden Xi Jinping ke Amerika Serikat, karena pada saat itulah China dan AS berhail mencapai kerjasama *cybersecurity* dalam *US-China Cyber Agreement 2015.* Selanjutnya adalah dialog bilateral tingkat tinggi dengan nama *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*, dan *U.S.-China Law Enforcement and Cybersecurity Dialogue*. Keduanya merupakan kerangka kerjasama *cybersecurity* sebagai bentuk kelanjutan dari kerjasama yang telah dicapai pada tahun 2015.

2.3.2 *National Interest*

Kepentingan nasional yang dibawa oleh diplomat merupakan Strategi dalam *cyberspace* suatu negara. Apabila melihat tujuan dari kebijakan luar negri, terdapat keselarasan antara tujuan yang ingin dicapai pemerintah dan juga tujuan dalam *cyberspace.* Selain itu, Strategi tersebut juga menyiratkan agenda diplomatik dalam

cyberspace. Negara memiliki nilai yang diperjuangkan dalam *cyberspace.* Strategi *cyberspace* kemudian menjadi pedoman suatu negara dalam mencapai tujuannya melalui *cyberdiplomacy*.

China meningkatkan perannya melalui hubungan diplomatik *cybersecurity* sebagai bentuk upaya mencapai kepentingannya dalam *cyberspace*. Inti dari *cyberdiplomacy* yang dilakukan oleh China adalah *cyber sovereignty* atau kedaulatan internet, yaitu kontrol dan manajemen atas konten internet.[73] Kedaulatan internet memiliki arti penting bagi pemerintah China yang berperan sebagai penyedia keamanan rakyat. *Cyber sovereignty* selanjutnya menjadi agenda diplomatik Strategi internasional dalam *cyberspace.*

Kepentingan nasional China dalam penelitian ini dilihat melalui *International Strategy of Cooperation on Cyberspace*. Untuk itu, pertama-tama penelitian ini menjelaskan isi dari Strategi tersebut. Tujuan Strategis partisipasi China dalam kerjasama *cyberspace* internasional adalah: melindungi kedaulatan negara, keamanan nasional, dan kepentingan pembangunan dalam *cyberspace*; memastikan keamanan arus informasi dalam internet; mempertahankan perdamaian, keamanan dan stabilitas dalam *cyberspace*; dan meningkatkan hukum yang berlaku dalam *cyberspace*.[74]

Setelah menjelaskan isi dari Strategi kerjasama, penelitian ini kemudian berupaya menganalisis kerjasama *cybersecurity* antara China dan AS menggunakan

[73] Niels Nagelhus Schia and Lars Gjesvik, *China's cyber sovereignty*, The Norwegian Institute of International Affairs (2017), p. 1.
[74] The State Council Information Office of the People's Republic of China, *International Strategy of Cooperation on Cyberspace*, 2017, <www.scio.gov.cn/32618/Document/1543874/1543874.htm> [accessed 8 April 2018].

Strategi tersebut. Selain tujuan, dokumen tersebut juga berisi posisi China dan kebijakan dalam isu *cyber* internasional, prinsip, dan rencana aksi untuk mewujudkan setiap tujuan dalam *cyberspace.*[75] Dengan begitu, diketahui bahwa kerjasama *cybersecurity* China-AS merupakan implementasi salah satu tujuan yang ingin dicapai China dalam *cyberspace.*

2.3.3 *Cyber Issue*

Isu *cyber* dalam hubungan suatu negara dapat memiliki berbagai macam bentuk. Dalam penelitian ini, isu *cyber* yang menjadi fokus penelitian adalah isu *cyber* internasional. Hal itu disebabkan oleh celah ancaman *cyberspace* bagi keamanan nasional yang dapat menyerang sewaktu-waktu dan tidak terduga. Isu yang diangkat menjadi aspek isu *cyberspace* internasional mengandung unsur politik dan tidak hanya bersifat teknis, sehingga kerjasama adalah sesuatu yang diperlukan oleh semua pihak.[76] Tercapainya sebuah kerjasama dapat menjadi awal dari perkembangan hubungan di bidang *cyberspace* dan isu *cyber* itu sendiri dalam tata kelola internet.[77]

Untuk mendapatkan pandangan terhadap isu *cyber* dalam kerjasama *cybersecurity* yang dicapai oleh China dan AS pada tahun 2015, penelitian ini melihat *cyber agenda* yang dibawa pada setiap pertemuan kedua belah pihak. Penelitian ini pertama menganalisis agenda diplomatik dalam *US-China Cybersecurity Dialogue.* Pada saat itu, bahkan kedua belah pihak memiliki *joint statement* sebagai hasil diskusi yang dipublikasikan pada tahun 2012.

---

[75] Ibid.
[76] Barrinha & Renard, Loc.cit., p. 30.
[77] Klimburg, Op. cit., p. 30

Selanjutnya penelitian ini menganalisis agenda dalam *U.S.-China Strategic and Economic Dialogue.* Seperti yang disebutkan sebelumnya, penelitian ini berfokus pada dialog S&ED yang kelima. Agenda dalam S&ED pada pertemuan kelima ini meliputi beberapa isu Strategis, yang diantaranya adalah peningkatan kerjasama bilateral, tantangan regional dan global, dialog bilateral dalam isu energy, lingkungan dan teknologi, bentuk kerjasama sub-nasional, dan bentuk-bentuk kerjasama dalam berbagai bidang lainnya. Diantara berbagai bentuk agenda, penelitian ini berfokus pada agenda yang berhubungan dengan ranah *cybersecurity.*

Penelitian ini lalu menjelaskan *cyber agenda* yang terdapat dalam kunjungan kenegaraan Presiden Xi Jinping ke Amerika Serikat, dan diteliti melalui hasil perbincangan kedua tokoh negara. Selain itu, penelitian ini turut menjelaskan agenda yang terdapat dalam laporan hasil *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues,* dan *U.S.-China Law Enforcement and Cybersecurity Dialogue.* Setelah melihat agenda dalam setiap pertemuan, penelitian ini kemudian berupaya mengidentifikasi isu *cyber* apa saja yang terdapat dalam agenda tersebut berdasarkan isu *cyber* pada umumnya, yaitu *cybersecurity, cybercrime, confidence-building,* kebebasan berinternet dan tata kelola internet.[78]

2.3.4 *Diplomat*

Diplomat dalam penelitian ini menjelaskan siapa saja representasi negara yang membawa agenda diplomatik dalam forum bilateral untuk mencapai kerjasama *cybersecurity* yang dilakukan oleh China dengan AS. Pertemuan bilateral tersebut antara lain adalah *US-China Cybersecurity Dialogue, U.S.-China*

[78] Barrinha & Renard, Loc.cit. p.3.

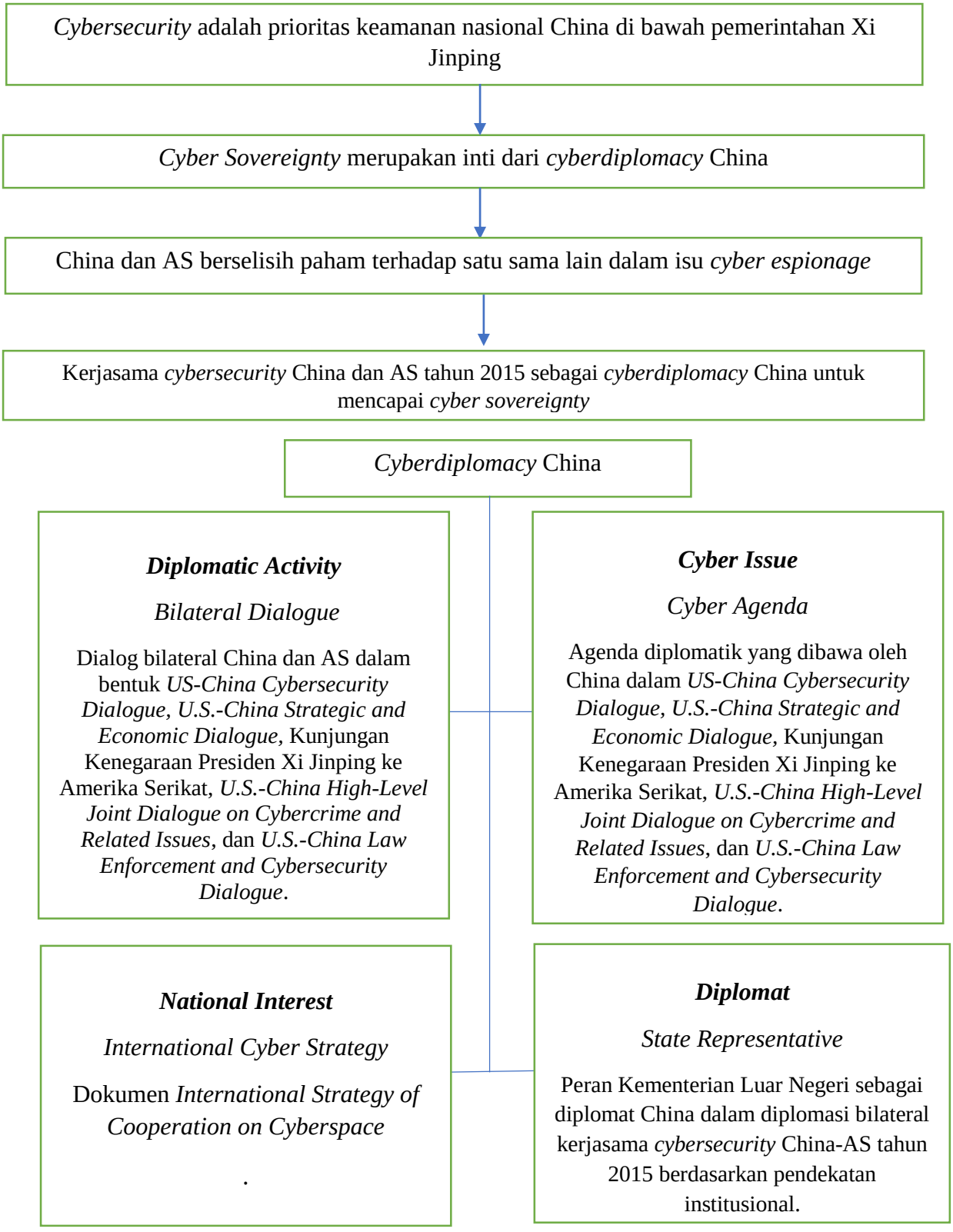
Strategic and Economic Dialogue, U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues, dan *U.S.-China Law Enforcement and Cybersecurity Dialogue*. Selain dialog, penelitian ini melihat perwakilan negara pada saat kunjungan kenegaraan Presiden Xi Jinping ke Amerika Serikat. Dari seluruh representasi negara dalam forum bilateral yang telah disebutkan, penelitian ini kemudian menganalisis peran KLN sebagai representasi negara. Sebelumnya masuk ke dalam peran KLN dalam forum bilateral, penelitian ini terlebih dahulu menjelaskan pendekatan institusional dengan berfokus pada peran KLN dalam struktur pemerintahan China.

Untuk mempermudah penelitian mengenai *Cyberdiplomacy* China melalui kerjasama *cybersecurity* China-AS tahun 2015, maka saya membuat operasionalisasi seperti di bawah ini:

Model	**Variabel**	**Indikator**	**Operasionalisasi**
Cyberdiplomacy	***Diplomatic Activity***	*Bilateral/ Multilateral Dialogue*	Dialog bilateral China dan AS dalam bentuk *US-China Cybersecurity Dialogue*, *U.S.-China Strategic and Economic Dialogue*, Kunjungan Kenegaraan Presiden Xi Jinping ke Amerika Serikat, *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*, dan *U.S.-China Law Enforcement and Cybersecurity Dialogue*.

	National Interest	*International Cyber Strategy*	Dokumen *International Strategy of Cooperation on Cyberspace* berisi tujuan dari kerjasama internasional China dalam *cyberspace.*
	Cyber Issue	*Cyber Agenda*	Agenda diplomatik yang dibawa oleh China dalam *US-China Cybersecurity Dialogue, U.S.-China Strategic and Economic Dialogue*, Kunjungan Kenegaraan Presiden Xi Jinping ke Amerika Serikat, *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*, dan *U.S.-China Law Enforcement and Cybersecurity Dialogue*.
	Diplomat	*State Representative*	Peran Kementerian Luar Negeri sebagai perwakilan negara China dalam diplomasi bilateral kerjasama *cybersecurity* China-AS tahun 2015 berdasarkan pendekatan institusional.

2.4 Kerangka Pemikiran



2.5 Argumen Utama

Cyberdiplomacy China dilihat melalui aktivitas diplomatik yang dilakukan oleh China untuk menangani permasalahan *cybersecurity* dengan AS, *national interest* berdasarkan dokumen Strategi kerjasama China dalam *cyberspace*, *cyber issues*, yaitu isu-isu dalam konteks *cyber* yang diangkat dalam aktivitas diplomatik tersebut, dan *diplomat* sebagai representasi negara yang membawa kepentingan politik. Argumen utama penulis dalam penelitian *cyberdiplomacy* China adalah kerjasama *cybersecurity* China-AS tahun 2015 merupakan langkah awal dari Strategi China untuk mencapai *cyber sovereignty*. Sesuai dengan politik luar negerinya dalam *cyberspace*, China berupaya untuk meningkatkan kerjasama *cybersecurity*. Dengan mencapai kerjasama *cybersecurity* dengan AS, China mendorong *cyber sovereignty* sebagai nilai dari tata kelola internet global.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini menggunakan jenis penelitian deskriptif. Melalui penelitian deskriptif, peneliti berusaha untuk menjelaskan berbagai macam fenomena yang ada, yang bersifat alamiah maupun buatan.[79] Fenomena yang terjadi dapat berupa aktivitas, karakteristik, perubahan, hubungan, kesamaan, dan perbedaan antara fenomena yang satu dengan yang lainnya.[80]

3.2 Ruang Lingkup Penelitian

Ruang lingkup penelitian ini adalah *cyberdiplomacy* China melalui kerjasama *cybersecurity* China-AS dalam kurun waktu 2013-2017. Rentang waktu penelitian berada pada tahun 2013-2017. 2013 dipilih karena pada tahun tersebut China mulai berfokus pada *cybersecurity* terhitung sejak Kongres Partai Nasional ke-18 diikuti dengan meningkatnya perselisihan hubungan *cybersecurity* China dan AS. Sedangkan tahun 2017 merupakan tahun dimana China dan AS telah mencapai kerangka kerjasama yang signifikan dalam bentuk LECD. Selain itu, penelitian ini berfokus pada *cyberdiplomacy* China melalui upaya diplomasi bilateral. Sudut pandang penelitian ini digunakan sudut pandang negara China.

[79]DR. Lexy Moleong, M.A., *Metodologi Penelitian Kualitatif* (Bandung: PT Remaha Rosdakarya, 2006), p. 17.
[80]Sukmadinata, *Metode Penelitian Pendidikan*. (Bandung:Rosdakarya, 2006), p. 72.

3.3 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan peneliti menggunakan studi pustaka. Peneliti menggunakan suber-sumber dokumen sebagai pengajian data mengenai fenomena yang dikaji. Data primer maupun sekunder dikumpulkan dan diolah hingga mencapai kesimpulan akhir. Data primer berupa data yang diperoleh langsung dari sumber yang dapat mempertanggungjawabkan validitas informasi yang diberikan, seperti pernyataan formal pemerintah melalui situs resmi pemerintah dan sumber berita internasional. Data sekunder didapatkan melalui literatur tertulis yang berkaitan dengan penelitian ini seperti buku, jurnal, dokumen kebijakan negara, situs berita dan artikel.[81]

Penulis mencoba mendapatkan sumber informasi di banyak tempat melalui berbagai sumber terbuka untuk mendapatkan data penelitian dan sumber informasi yang lebih akurat. Lokasi rujukan penulis untuk melakukan kegiatan penelitian diantaranya adalah:

1. Ruang baca jurusan Hubungan Internasional Universitas Brawijaya
2. Perpustakaan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Brawijaya
3. Perpustakaan Pusat Universitas Brawijaya
4. Ruang baca jurusan Hubungan Internasional Universitas Muhammadiyah Malang
5. Perpustakaan Fakultas Ilmu Sosial dan Ilmu Politik Universitas Airlangga
6. Perpustakaan Pusat Universitas Indonesia

[81]Moleong, Op.Cit., pp. 234-235.

3.4 Teknik Analisa Data

Penelitian ini adalah jenis penelitian kualitatif. Proses analisis data dimulai dengan menelaah seluruh data yang didapat dari berbagai sumber. Data-data tersebut dibaca, dipelajari, dan ditelaah untuk mereduksi data dengan cara abstraksi. Abstraksi merupakan rangkuman inti yang memuat proses dan pernyataan-pernyataan yang relevan dalam menyusun hasil penelitian. Setelah itu data yang didapatkan dielaborasikan dengan fakta yang ada dan dijelaskan kembali dalam bentuk untuk mendapatkan kesimpulan yang mendalam. Tahap akhir dari analisis data adalah melakukan evaluasi yaitu pemeriksaan validitas data.[82]

3.5 Sistematika Penulisan

Untuk memudahkan pemahaman alur pemikiran dalam penulisan ini, sistem penulisan dibagi menjadi kedalam 6 bab yang masing-masing terdiri atas beberapa sub bab. Sistematika penulisan adalah sebagai berikut:

BAB I : PENDAHULUAN

Bab I memuat bagian pendahuluan yang berisi latar belakang masalah, rumusan masalah, dan tujuan serta manfaat penelitian

BAB II : KAJIAN PUSTAKA

Bab II memuat bagian metodologi berisi penelitian terdahulu untuk membandingkan dan mencari knowledge gap yang ada, kerangka konseptual sebagai dasar yang membantu dalam membangun logika dalam menjawab rumusan

[82]Moleong, *Op.cit.*, hal. 245.

masalah atas pertanyaan penelitian, operasionalisasi konsep, kerangka berpikir, dan argumen utama.

BAB III : METODE PENELITIAN

Bab III berisi metode penelitian, yakni penjelasan alur penelitian yang terdiri atas jenis penelitian, ruang lingkup penelitian, teknik pengumpulan data, tenik analisa data, dan sistematika penulisan.

BAB IV : GAMBARAN UMUM

Bab IV menjelaskan bagian gambaran umum mengenai kebijakan *cybersecurity* China, mulai dari esensialitas *cybersecurity* bagi China, kebijakan politik luar negri di bawah pemerintahan presiden Xi Jinping. Lalu bagaimana perkembangan *cyberdiplomacy*, upaya *cyberdiplomacy* China, hingga permasalahan dalam hubungan *cyber*security China-AS.

BAB V: *CYBERDIPLOMACY* CHINA TERHADAP AMERIKA SERIKAT TAHUN 2013-2017

Bab V menjabarkan *cyberdiplomacy* China terhadap AS tahun 2013-2017 menggunakan operasionalisasi konsep *cyberdiplomacy* yang ditulis oleh Andre Barrinha dan Thomas Renard.

BAB VI PENUTUP

Bab VI berisi tentang kesimpulan dari hasil penelitian dan saran guna penelitian lebih lanjut.

BAB IV

GAMBARAN UMUM

Bab ini berisi gambaran umum mengenai objek penelitian yaitu *cyberdiplomacy* yang dilakukan oleh pemerintah China. Dalam hubungan *cybersecurity* China-AS terdapat permasalahan keamanan spionase siber yang terjadi di antara keduanya.

4.1 Politik Luar Negeri China di bawah pemerintahan presiden Xi Jinping

Di bawah pemerintahan Xi Jinping, politik luar negri China bersifat asertif.[83] Hal ini menandakan bahwa China lebih percaya diri dalam perpolitikan internasional, dan secara aktif berperan penting di dalamnya. China berupaya menunjukkan bahwa ia mampu sebagai kekuatan internasional. Dalam kebijakan yang diambil maupun implementasinya, China terlihat lebih tegas dibandingkan dengan gaya politik luar negri pemerintah sebelumnya.[84] Ketegasan China terlihat dari bagaimana China menggaungkan prinsip kedaulatan dan non-intervensi, begitu juga dengan membela kedaulatan teritori dalam sengketa maritimnya.[85]

Politik luar negri China dikenal dengan *peaceful development,* sebuah orientasi politik luar negri dimana China mulai bangkit secara perlahan menjadi negara yang kuat dengan tetap menjunjung perdamaian antar negara.[86] China

[83] Jian Zhang, 'China's new foreign policy under Xi Jinping: towards 'Peaceful Rise 2.0'?', *Global Change, Peace & Security*, 27:1, (2015), pp. 5-19 (p. 5).
[84] Ibid, p. 7.
[85] Directorate-General for External Policies European union, *China's foreign policy and external relations*, (2015) p. 13.
[86] Ibid.

kemudian meningkatkan kerjasama internasional sebagai bentuk pembangunan yang damai. Tetapi, perdamaian versi China bukanlah perdamaian tanpa syarat. China tetap mengutamakan kepentingan nasionalnya sebagai hal fundamental dalam setiap kebijakan, terutama dalam hubungannya dengan negara lain. Komitmen terhadap perdamaian bagi China berada pada kondisi dimana pihak lainnya dapat memberikan timbal balik yang menguntungkan bagi kepentingan China.[87] Perdamaian secara politik digunakan China untuk membangun stabilisasi dalam sebuah kondisi eksternal yang dapat mendukung kebangkitan China sebagai kekuatan global.

Walaupun bersifat asertif dan keras, China memiliki kecenderungan untuk tidak melakukan intervensi terhadap politik dalam negeri negara lain. Cara China untuk mengambil hati adalah dengan secara aktif berperan dalam dunia internasional tanpa berupaya terlihat sebagai kekuatan hegemoni.[88] China sangat berpegang teguh pada prinsip kedaulatan dalam politik luar negerinya. Prinsip tersebut digunakan untuk mempertahankan kesatuan teritori dan yurisdiksi pemerintah China atas teritori tersebut.[89] China menghimbau negara lainnya untuk menghormati kedaulatan setiap negara. Melalui prinsip kedaulatan, China berupaya untuk memperjuangkan hak negara berkembang yang seringkali mendapatkan intervensi dari negara lain.

Di bidang keamanan, kebijakan asertif China sangat terlihat dalam peran China sebagai aktor penjaga stabilitas kawasan Asia Pasifik. Hal ini dilakukan

[87] Ibid., p. 11.
[88] Abraham M. Denmark, 'US Strategic Rebalancing and China's Rise', in Mingjiang Li & Kalyan M. Kemburi (Ed.), *New Dynamics in US–China Relations* (Routledge, 2015), p. 23.
[89] Jian Zhang, Loc. Cit, p. 16.

China sebagai respon terhadap meningkatnya kehadiran AS di kawasan Asia.[90] China begitu keras mempertahankan kedaulatan maritimnya dalam Sengketa Laut China Selatan maupun Kepulauan Senkaku. Tetapi, China tidak pernah sampai menggunakan kekerasan sebagai jalan keluar.

Xi Jinping menggunakan dua bentuk konsep hubungan luar negeri dalam politik luar negerinya. Pertama adalah "*New Type of Major Power Relations*", yang merupakan bentuk hubungan baru antara China dan AS. Konsep tersebut mengandung makna bahwa negara dengan kekuatan dominan pada saat ini yaitu AS, dan negara *rising power* yaitu China dapat terhindar dari perang dengan melakukan peningkatan kerjasama dalam hubungan China-AS.[91]

Bentuk hubungan yang kedua adalah *"Community of a Common Destiny',* yang menunjukkan bahwa China, seperti halnya berbagai negara di dunia, menuju sebuah keinginan dan nasib yang sama. Tujuannya adalah untuk memperkuat ikatan hubungan antara China dengan negara lainnya.[92] Dalam *cyberspace*, Xi Jinping membangun konsep hubungan antar negara yang disebut dengan *"a cyberspace community of common destiny"*. Konsep tersebut menekankan pada tantangan yang diberikan oleh internet pada saat ini menjadikan kerjasama antar negara dalam *cyberspace* merupakan suatu kebutuhan.[93]

[90] Denmark, Loc. Cit., p. 20.
[91] Dingding, Loc.cit.
[92] Jian Zhang, Loc. Cit, p. 14.
[93] Huaxia, 'President Xi stresses int'l cooperation in cyberspace governance', *Xinhua*, <http://www.xinhuanet.com/english/2016-11/16/c_135834559.htm> [accessed 20 November 2017].

4.1.1 Kebijakan luar negeri *cybersecurity* China

Politik asertif China juga terlihat dalam ranah *cyberspace.* Dalam isu *cybersecurity*, China banyak mengambil peran penting melalui tata kelola internet, terutama dalam membentuk norma perilaku *cyberspace*. Salah satu bentuknya adalah ketika Presiden Xi kemudian berambisi menjadikan China sebagai *cyberpower* sejak tahun 2014. *"Efforts should be made to build our country into a cyber power"*[94], dinyatakan oleh Xi Jinping dalam pertemuan pertama *the Internet Security and Informatisation Leading Small Group* (ISILSG), atau yang sekarang dikenal dengan *Office of the Central Cyber Security and Informatization Commission* (OCCSIC), sebuah *working group* di bidang cybersecurity dan keamanan informasi yang dipimpinnya. Membangun kekuatan internet dengan teknologi informasi yang kuat dan layanan informasi komprehensif, masyarakat berbudaya internet, membangun ekonomi informasi, dan jaringan berkualitas tinggi adalah tujuan-tujuan yang ingin dicapai Xi Jinping untuk kesejahteraan rakyat China.[95]

Selain menjadi kekuatan internet, kedaulatan merupakan bagian dari kepentingan nasional China yang juga berwujud sebagai teritori *cyberspace.*[96] China secara aktif menyuarakan ideologinya mengenai kedaulatan internet, dan menjalin kerjasama internasional terkait *cybersecurity* dengan negara lainnya. Hal

[94] The Cyberspace Administration of China, *The first meeting of the Central Network Security and Informatization Leading Group held an important speech by Xi Jinping,* 2014, <http://www.cac.gov.cn/2014-02/27/c_133148354.htm> [accessed 16 June 2018].
[95] Ibid.
[96] Ye Zheng, 'From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond', in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, (eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, (Oxford University Press, 2015), p. 132.

tersebut sesuai dengan politik luar negri China yang mengedepankan kerjasama yang damai.

Kebijakan luar negri China memiliki tiga tujuan utama terkait *cyberspace.* Pertama, mencegah dan mengatasi ancaman yang ditimbulkan oleh internet terhadap keamanan dan stabilitas rezim CCP. Kedua, membangun *cyberspace* sebagai ranah pengaruh secara ekonomi, politik, dan militer bagi China. Ketiga, menandingi kemajuan kekuatan *cyber* AS sambil memberikan ruang bagi China untuk menjadi lebih unggul.[97] Untuk mencapai tujuan-tujuannya, China berpartisipasi dalam pemerintahan global melalui tata kelola internet secara multilateral maupun bilateral yang diwujudkan melalui *cyberdiplomacy.*

Wujud implementasi politik luar negeri China dalam *cyberspace* terlihat dari berbagai kebijakan yang diambil terutama mengenai kerjasama *cybersecurity.* China terlebih dahulu mendorong kedaulatan *cyberspace* melalui draft *International Code of Conduct for Information Security.* Bersama dengan Rusia, Tajikistan dan Uzbekistan, China membentuk lalu menyerahkan draft tersebut ke PBB pada tahun 2011. Hal itu menunjukkan ketegasan China dalam membentuk norma *cyberspace* mengingat pada saat itu, AS dan Inggris tengah bersiap untuk melakukan hal yang sama melalui Konferensi London tahun 2011.[98]

China meningkatkan kerjasama *cybersecurity* dengan negara lainnya. Secara keseluruhan, China telah melakukan kerjasama *cybersecurity* sebanyak 23 kali dengan 15 bentuk kerjasama bilateral dengan 12 negara dan 8 kerjasama

[97] Adam Segal, 'Chinese Cyber Diplomacy in a New Era of Uncertainty', *Hoover Working Group on National security, Technology, and Law*, Aegis Paper Series No. 1703, (Stanford University, 2017), p. 1.
[98] Ibid., p. 5.

multilateral.[99] Kerjasama *cybersecurity* yang dicapai China adalah kerjasama antara China dan Rusia pada tahun 2015. China dan Rusia berada pada posisi yang sama terkait *cyber sovereignty,* sehingga tidak banyak pertentangan dalam mencapai sebuah kesepakatan. Kerjasama tersebut menekankan pada non agresi dalam *cyberspace*, bahwa kedua belah pihak dilarang untuk melakukan serangan *cyber* dalam bentuk apapun, dan juga menghormati kedaulatan masing-masing.[100]

Di tahun yang sama, China menyepakati kerjasama *cybersecurity* dengan AS. Perbedaan kerjasama *cybersecurity* yang dilakukan China dengan AS jika dibandingkan dengan Rusia terletak pada penekanan terhadap aktivitas spionase siber. Kerjasama ini merupakan pertama kalinya spionase siber diatur sebagai aktivitas yang dilarang dalam *cyberspace* melalui kesepakatan bilateral. China kemudian mengembangkan hubungan bilateralnya dalam bidang *cybersecurity* dengan negara barat lainnya seperti Inggris pada tahun 2016, Pernyataan Bersama China- Australia pada tahun 2017, dan mencapai kesepakatan *cybersecurity* dengan Jerman pada tahun 2016.[101] Secara garis besar, kesepakatan tersebut diantaranya berisi mengenai larangan pencurian hak kekayaan intelektual, dan pembentukan mekanisme untuk melawan terorisme, *cyber crime*, dan ancaman *cyber* lainnya.

---

[99] Theresa Hitchens & Nilsu Goren, *International Cybersecurity Information Sharing Agreements*, (Center For International and Security Studies at Maryland, 2017), p. 11.

[100] Russian Federation, *Order of the Russian Government on signing the agreement between the government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of ensuring international information security*, 2015, <https://*cyber*-peace.org/wp-content/uploads/2013/05/RUSCHN_*Cyber*SecurityAgreement201504_InofficialTranslation.pdf> [accessed 10 August 2018].

[101] Hitchens & Goren, Loc.cit., p. 12.

4.1.2 Kebijakan domestik *cybersecurity* China

China adalah negara dengan sistem pemerintahan otoriter dengan struktur yang tersentralisasi pada satu partai, yaitu Partai Komunis China atau *Chinese Communist Party* (CCP). Pemerintah secara berdaulat memiliki kewenangan atas rakyat China. Kepentingan utama pemerintah China adalah mempertahankan keberlangsungan kekuasaan CCP dengan memperoleh dukungan rakyat. [102] Segala kebijakan *cybersecurity* serta visi dan misinya berada di bawah kebijakan CCP.

Dalam rencana pembangunannya, China berupaya untuk meningkatkan *cybersecurity* dengan mengembangkan teknologi, membangun sistem informasi, dan juga membentuk jaringan tata kelola internet dalam struktur pemerintahannya. Hal tersebut tercermin dari rencana pembangunan China dalam Dokumen Rencana 5-tahun ke-13 yang berbunyi sebagai berikut,

> "*We will strengthen anti-espionage work. We will step up our struggle against hostile forces concerning cyberspace sovereignty, strengthen guidance on online public discourse, and work to prevent hostile and terrorist forces from carrying out infiltration and sabotage activities in cyberspace*." [103]

Dokumen tersebut menjelaskan bahwa dalam rencana pembangunan 5 tahun Cina, terlihat upaya Cina memerangi spionase maupun *cybercrime* dan melindungi keamanan rakyat Cina dalam *cyberspace*. Hal tersebut selaras dengan

[102] Cheng Li, "China's Communist Party-State: The Structure and Dynamics of Power," in William A. Joseph, (eds.), *Politics in China An Introduction* (New York: Oxford University Press, 2014), p. 192.
[103] Central Committee of the Communist Party of China Beijing, *The 13th Five-Year Plan For Economic And Social Development Of The People's Republic Of China (2016–2020)*, pp. 75-80 (2016), China Central Compilation & Translation Press <http://en.ndrc.gov.cn/newsrelease/201612/P020161207645765233498.pdf> [accessed 24 November 2017].

poin kerjasama *cybersecurity* Cina-AS dimana salah satu poin yang disepakati diantaranya adalah melawan *cybercrime,* spionase dan *cyberterrorism.*

Pentingnya *cybersecurity* tidak dapat dilihat melalui satu sisi saja. *Cybersecurity* telah terintegrasi dalam berbagai bidang, terutama di bidang ekonomi dan keamanan. Saat ini, China berada dalam masa transisi menjadi negara berbasis industri dan teknologi informasi, dimana pemerintah menggenjot kemajuan teknologi sebagai pondasi utama roda perekonomian.[104] Ekonomi digital bahkan telah memberikan kontribusi sebanyak 30% dalam pencapaian GDP China pada tahun 2016.[105]

Tetapi kemudian perkembangan teknologi informasi juga menjadi ancaman bagi pemerintah. Kepentingan utama bagi partai CCP adalah menjaga stabilitas sosial dan politik.[106] *Cyberspace* membuka celah ancaman bagi pemerintah, dimana ancaman tersebut tidak hanya berasal dari domestik, tetapi juga internasional. Segala aktivtias anti-pemerintah maupun provokasi menggunakan *cyberspace* dengan tujuan mengacaukan situasi domestik, aksi penyebaran kebencian dan terorisme, dan juga separatis yang mengancam kedaulatan teritorial China adalah ancaman utama yang dihadapi pemerintah.[107] Begitu juga dengan aksi kriminal menggunakan *cyberspace.* Berdasarkan laporan Xinhuanet tahun 2016, polisi

---

[104] Cuihong Cai, 'Cybersecurity in Chinese Context: Changing Concepts, Vital Interests, and Cooperative Willingness,' (paper presented at 9th Berlin Conference on Asian Security (BCAS), June 14-16, 2015), p. 13. <https://www.swp-berlin.org/fileadmin/contents/projects/BCAS2015_Cai_Cuihong_Web.pdf> [accessed 11 February 2017].

[105] Xinhua, *China's digital economy accounts for 30% of 2016 GDP: Report*, 2017, <http://www.chinadaily.com.cn/business/4thwic/2017-12/05/content_35212111.htm> [accessed 24 November 2017].

[106] Amy Chang, *Warring State: China's Cybersecurity Strategy*, (Center for a New American Security, 2014), p. 12.

[107] Cai, Op.Cit., p. 12.

berhasil menangkap 19.349 jumlah kasus penipuan *cyber*[108] dan 710 kasus kejahatan online pada awal tahun 2017, dengan tingkat kenaikan pelaku kriminal dalam *cyberspace* sebanyak 80.7% dalam 1 tahun.[109] Angka tersebut dirasa cukup banyak, karena sulit untuk mengidentifikasi semua jenis serangan *cyberspace.* Terlebih lagi, jumlah serangan yang teridentifikasi belum mencakup perhitungan semua jenis kejahatan *cyber*.[110]

Sedangkan kasus internasional berasal dari kelemahan China dalam menghadapi serangan *cyber* yang dilakukan oleh negara lainnya. Ancaman tersebut terutama berasal dari penggunaan teknologi barat. Salah satu kasus besar yang menimpa China adalah diketahuinya aktivitas Badan Keamanan Nasional oleh AS yang melakukan pengambilan data secara rahasia melalui pembuatan 'jalur belakang' pada jaringan perangkat keras.[111] Karena, sistem operasi dalam suatu perangkat dapat digunakan sebagai celah untuk meretas informasi perangkat tersebut. Pemerintah China kemudian berupaya untuk mengembangkan teknologi informasi dengan produknya sendiri sebagai antisipasi serangan *cyber* dan membangun kapabilitas *cyber.*

Pemerintah China berperan besar untuk mengimbangi keberlangsungan kegiatan perekonomian, dan juga menjaga keamanan warga negaranya. Penggunaan *cyberspace* dikontrol melalui regulasi dan implementasi kebijakan

---

[108] Xinhua, *Procuratorates approve arrest of 19,000 telecom fraud suspects*, 2017. <http://news.xinhuanet.com/english/2017-01/14/c_135982423.htm> [accessed 29 July 2018].

[109] Xinhua, *Online crime continues to rise in China*, 2017, <http://www.chinadaily.com.cn/china/2017-10/16/content_33329294.htm> [accessed 9 February 2018].

[110] Greg Austin, C*ybersecurity in China The Next Wave,* (Springer, 2018), p. 83.

[111] China Daily USA, *US should 'explain hacking activity'*, 2013, <http://usa.chinadaily.com.cn/epaper/2013-06/14/content_16621289.htm> [accessed 14 February 2018].

cybersecurity. Ketika menjabat pada tahun 2013, presiden Xi Jiping menekankan kemajuan pada beberapa aspek dalam pemerintahannya, diantaranya adalah *cybersecurity*. *"No national security without cybersecurity, and no modernization without informationization*"[112], Xi Jinping menekankan pentingnya *cybersecurity* sebagai agenda politik utama dan menjadikan *cyber* sebagai prioritas Strategi nasional yang berimplikasi pada militer, politik, dan ekonomi.[113]

Perhatian China terhadap *cybersecurity* mulai terlihat sejak Kongres Nasional ke-18 dan ditekankan kembali pada Kongres Nasional ke-19.[114] *Cybersecurity* telah menjadi ranah penting bagi keamanan dan pertahanan China terutama dalam hal pengembangan kapabilitas militer. "*We should attach great importance to maritime, space and cyberspace security"*[115], selain ranah maritim dan ruang angkasa, *cybersecurity* memegang peran penting dalam keamanan nasional China. Disebutkan pula sikap China dalam perpolitikan internasionalnya terkait *cyberspace,* bahwa China akan mengutamakan kepentingan nasionalnya terutama terkait kedaulatan China dalam bentuk apapun, menyelesaikan konflik terkait *cyberspace* melalui dialog secara damai, dan secara aktif berperan dalam pemerintahan global.[116]

---

[112]Xinhuanet, *The First Meeting of the Central Cyber Security and Informationization Leading Group Held an Important Speech by Xi Jinping*, 2014, <http://www.cac.gov.cn/2014-02/27/c_133148354.htm> [accessed 24 July 2018].
[113] Cai, Loc.cit.
[114] Li Yuxiao & Xu Lu, 'China's Cybersecurity Situation and the Potential for International Cooperation', Op.Cit., p. 229.
[115] Embassy of the People's Republic of China in the United States of America, *Full text of Hu Jintao's report at 18th Party Congress*, 2012, <http://www.china-embassy.org/eng/zt/18th_CPC_National_Congress_Eng/t992917.htm> [accessed 29 February 2017]
[116] *Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era (Delivered at the 19th National Congress of the Communist Party of China October 18, 2017),*

Untuk menjaga stabilitas domestik, pemerintah China memiliki beberapa kebijakan terkait *cybersecurity.* Pertama adalah *the Great Firewall of China*. Pemerintah China mengontrol setiap aktivitas *cyber* yang masuk maupun keluar dari China. Tidak hanya itu, mereka juga melakukan sensor dan kontrol atas konten internet.[117] Sedangkan untuk keamanan dan pertahanan *cyberspace,* pemerintah China memiliki pasukan intelijen yang dinamakan dengan *patriot hacker.* Mereka adalah kelompok peretas yang direkrut pemerintah untuk melakukan peretasan sistem informasi dengan target internasional.[118] Sedangkan kebijakan China yang baru saja diberlakukan adalah *cybersecurity law*. Melalui *cybersecurity law*, pemerintah dapat melakukan kontrol terhadap data yang dimiliki oleh perusahaan domestik maupun internasional yang ada di wilayah China.[119]

Strategi *cybersecurity* China di bidang militer tertulis dalam berbagai *White Paper* atau buku putih yang dikeluarkan oleh pemerintah. Meskipun mengalami banyak perkembangan, *cybersecurity* tetap menjadi poin penting didalamnya. *White Paper* pertama yang menyebutkan *cybersecurity* diterbitkan pada 8 Juni 2010 oleh Kantor Informasi Dewan Negara China, dan disebut dengan *White Paper on the internet in China*. Dokumen tersebut berisi penjelasan mengenai *cybersecurity* dan peran pemerintah sebagai pemegang otoritas tertinggi yang meregulasi penggunaan internet. "*Within Chinese territory the Internet is under the jurisdiction*

<http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf> [accessed 24 July 2018].
[117] Austin, Loc.cit., p. 12
[118] Nigel Inkster, 'Cyber Espionage', in *China's Cyber Power,* Adelphi Series, Vol. 55, No. 456, (2015), pp. 51-82 (p. 67).
[119] Caitríona H. Heinl, 'New Trends in Chinese Foreign Policy: The Evolving Role of Cyber', *Asian Security*, (2017), p. 4.

of chinese sovereignty. The Internet sovereignty of China should be respected and protected".[120] Di dalam teritori wilayah China, penggunaan internet berada dibawah yurisdiksi pemerintah, dimana kedaulatan internet menjadi bagian penting didalamnya. *White Paper* kedua adalah Strategi militer yang dipublikasikan pada tahun 2015. *Cyberspace* disebutkan sebagai salah satu ranah komando terpenting dalam kekuatan militer China , dan juga merupakan salah satu dari domain strategis seperti maritim, ruang angkasa, dan kekuatan nuklir.[121]

4.2 Keterbukaan informasi dan teknologi asing sebagai ancaman terhadap *cybersecurity* China

Memahami ancaman *cybersecurity* bagi China berarti melihat ancaman tersebut dari sudut pandang negara China itu sendiri. Pemerintah China selalu berupaya untuk mempertahankan legitimasi partai CCP sebagai rezim yang berkuasa. Upaya tersebut dilakukan dengan mempertahankan stabilitas politik melalui kontrol informasi dan menekankan pada paham sosialisme sebagai dasar ideologi negara.[122] Ancaman bagi China kemudian adalah segala aktivitas *cyberspace* yang dapat membahayakan kedaulatan pemerintah China.

Keterbukaan informasi dapat menjadi celah bagi penetrasi ideology yang bertentangan dengan nilai dasar dan budaya dari masyarakat China. China

---

[120] Information Office of the State Council of the People's Republic of China, 'The Internet in China', *Xinhua*, 2010, <http://www.chinadaily.com.cn/china/2010-06/08/content_9950198_7.htm> [accessed 5 May 2018].
[121] The State Council Information Office of the People's Republic of China, *China's Military Strategy*, (2015), < http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm> [accessed 20 July 2018].
[122] Cai, Op.Cit., pp. 11-18.

menganggap bahwa internet merupakan alat transportasi yang diciptakan untuk membawa pengaruh dan nilai dari barat, dimana hal tersebut mengancam ideologi dan nilai yang dimiliki oleh rakyat China.[123] Informasi digunakan sebagai bahan bakar untuk memunculkan para oposisi politik dalam bentuk kelompok anti-pemerintah China yang didukung oleh pemerintah asing untuk menggulingkan partai CCP.[124] Selain itu, keterbukaan informasi dapat mendatangkan intervensi politik. China adalah negara yang memiliki perbedaan pemikiran dengan berbagai negara di dunia, sehingga China seringkali mendapatkan kritik internasional terutama mengenai permasalahan Hak Asasi Manusia.

Norma internasional mengenai Hak Asasi Manusia salah satunya menyebutkan bahwa negara bertanggungjawab untuk melindungi keamanan internet warga negaranya dan memberikan akses internet terhadap setiap orang. Sebagai bagian dari komunitas internasional, maka pemerintah China seharusnya memberikan privasi dan kebebasan berpendapat bagi warganya. Tetapi yang terjadi adalah sebaliknya. Pemerintah China justru mengontrol arus informasi dengan legitimasi bahwa hal tersebut ditujukan untuk keamanan warga negara China.[125]

Selain keterbukaan informasi, kerentanan yang ditimbulkan oleh *cyberspace* terhadap keamanan informasi berasal dari teknologi asing.[126] Perangkat

[123] Cai, Loc.cit.
[124] Jon R. Lindsay, 'The Impact of China on Cybersecurity', in *International Security*, Vol. 39, No. 3, (2014), p. 18.
[125] Sarah Mckune, 'Foreign Hostile Forces', in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, (eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, (Oxford University Press, 2015), pp. 260-261.
[126] Mikk Raud, *China and Cyber: Attitudes, Strategies, Organisation*, (NATO CCD COE, 2016), p. 6.

teknologi China maupun sistem informasi yang digunakan sebagian besar merupakan teknologi yang berasal dari barat. Pihak asing dapat membuat sebuah 'jalur belakang' dalam sistem informasi yang ada di wilayah China untuk mencuri informasi milik masyarakat China seperti yang terjadi dalam pemantauan *cyberspace*, serangan *cyber*, maupun pencurian informasi dan data. Data tersebut terdapat informasi mengenai pengembangan teknologi, tren sosial, keamanan nasional, dan informasi intelijen dan operasi militer China.[127] Sehingga penting bagi China untuk mengamankan data, seperti halnya keamanan nasional.

4.3 Perkembangan *Cyberdiplomacy*

Perkembangan teknologi telah dapat membawa dunia dalam genggaman setiap individu. Potensi ancaman kemudian muncul dari banyaknya celah yang dihasilkan oleh teknologi informasi. Negara sebagai penyedia keamanan mendapatkan tantangan besar untuk dapat menjaga keamanan negara maupun keamanan individu setiap warga negaranya. *Cyberspace* telah terintegrasi sebagai Strategi keamanan dan pertahanan, termasuk juga Strategi diplomasi yang digunakan suatu negara untuk menjaga keamanan nasionalnya. Meningkatnya jumlah serangan *cyber* melalui tindakan kriminal dengan motif ekonomi maupun politik, menimbulkan kekhawatiran diantara para pemimpin dunia.

Perbedaan kapabilitas dalam *cyberspace* dapat menyebabkan adanya kesenjangan antara negara yang kuat dan negara yang lemah. Minimnya kemampuan pertahanan *cyber* suatu negara yang tidak diimbangi dengan

[127] Cai, Loc.cit.

kemampuan diplomatik yang baik menyebabkan negara tersebut rentan untuk menjadi sasaran serangan *cyberspace.* Contoh kasus yang pernah terjadi adalah serangan *cyber* yang menimpa Georgia pada tahun 2008. Sebagai negara dengan kekuatan *cyber,* Rusia menyerang Georgia sebagai bentuk perlawanannya dalam konflik Rusia-Georgia dengan melumpuhkan seluruh sektor yang telah terintegrasi dengan teknologi informasi.[128] Selain Georgia, serangan *cyber* juga terjadi di Estonia pada tahun 2007 dan virus Stuxnet yang menyerang Iran pada tahun 2010.

Selain kecemasan mengenai keamanan nasional, timbul saling ketidakpercayaan antara pemimpin negara satu dengan yang lainnya, terutama apabila berkaitan dengan kontrol rezim suatu pemerintahan seperti halnya China dan Rusia. Pengawasan pemerintah melalui kontrol terhadap aktivitas internet menimbulkan kecurigaan adanya perintah langsung untuk melakukan serangan *cyber* yang ditujukan pada negara lainnya. Sehingga, selain meningkatkan pertahanan *cyber,* penting untuk melakukan Strategi diplomatik sebagai bentuk upaya meningkatkan kepercayaan diantara para pemimpin dunia melalui *cyberdiplomacy.*[129]

Strategi diplomasi dalam ranah *cyberspace* mulai menjadi perhatian pada dekade pertama abad 21, diikuti dengan munculnya Strategi nasional *cybersecurity* oleh negara dengan kekuatan *cyber*.[130] Literasi mengenai konsep *cyberdiplomacy* pada saat itu masih sangat minim. Strategi keamanan *cyberspace* hanya berfokus

---

[128] John Markoffaug, 'Before the Gunfire, Cyberattacks', *New York Times*, 2008, <https://www.nytimes.com/2008/08/13/technology/13cyber.html> [accessed 25 July 2018].
[129] Dana Danca, '*Cyber* Diplomacy — A New Component of Foreign Policy', *Journal of Law and Administrative Sciences*, Issue 3, (2015), pp. 93–97 (p. 92).
[130] André Barrinha & Thomas Renard, '*Cyber*-diplomacy: the making of an international society in the digital age', *Global Affairs* (2017), pp. 1-12, (p. 6).

pada keamanan domestik dan tidak mengarah pada Strategi dalam aspek internasional. Seiring dengan meningkatnya isu serangan *cyberspace* menyebabkan rasa ketidakamanan bagi setiap negara dan muncul perhatian internasional terkait *cybersecurity*.

Hingga pada tahun 2010 terbit literasi yang secara jelas menekankan unsur kebijakan luar negri mengenai diplomasi dengan agenda *cyberspace* sebagai isu utama. Studi yang diterbitkan oleh EastWest Institute menjelaskan *cyberdiplomacy* sebagai Strategi diplomatik yang dilakukan oleh AS dan Rusia dengan menggunakan pendekatan kebijakan luar negeri di bidang *cybersecurity*. Literasi lainnya ditemukan dalam Strategi *cyberspace* internasional milik AS tahun 2011, yang untuk pertama kalinya dokumen resmi negara mengeluarkan Strategi internasional menggunakan alat dan sumber daya diplomatik untuk mencapai kepentingan dalam *cyberspace*.[131] Sedangkan penggunaan kata *"cyberdiplomacy"* pertama kali digunakan dalam dokumen resmi negara dalam *Council Conclusions on Cyber Diplomacy* oleh anggota negara Uni Eropa pada tahun 2015.[132]

Perhatian internasional terkait *cyberspace* masih pada sebatas pembentukan norma dan perilaku.[133] Hal tersebut disebabkan oleh belum adanya istilah mengenai *cyberspace* yang digunakan secara universal. Menjadi tantangan tersendiri dalam keamanan internasional saat ini untuk membangun pemahaman bersama atas tolak ukur yang dapat digunakan sebagai parameter perilaku negara. Isu *cyber* kemudian

[131] Barrinha & Renard, Loc.cit., pp. 4-7.
[132] Barrinha & Renard, Op.cit.
[133] Heli Tiirmaa-Klaar, 'Cyber diplomacy: Agenda, challenges and mission', in K. Ziolkowski (Ed.), *Peacetime regime for state activities in cyberspace: International law, international relations and diplomacy* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), p. 546.

mengalami internasionalisasi melalui berbagai kegiatan diplomatik sebagai upaya untuk mencapai konsensus perihal norma perilaku *cyberspace* dan mempertahankan perdamaian. Dimulai dari isu *cybersecurity*, buah dari *cyberdiplomacy* dapat dilihat melalui kesepakatan yang diambil sebagai tujuan utama *cyberdiplomacy* itu sendiri. Untuk mencapai tujuan tersebut, inisiatif internasional yang telah terbentuk diantaranya adalah UN GGE dan *Global Conference on Cyberspace* (GCCS).[134]

4.4 Upaya *Cyberdiplomacy* China

Sesuai dengan politik luar negrinya yang lebih asertif, China secara proaktif membangun norma perilaku *cyberspace* melalui Strategi diplomasinya dalam forum multilateral maupun bilateral. Dalam forum multilateral, melalui berbagai konferensi dan institusi internasional, China secara tegas menyatakan aspirasinya mengenai *cybersecurity* dan mendukung kerjasama global. China bahkan menjadi tuan rumah dalam konferensi internasional mengenai tata kelola *cyberspace*. Secara bilateral, pemerintahan Xi Jinping menunjukkan adanya peningkatan dalam hal kerjasama *cybersecurity* yang dilakukan China dengan negara lainnya.

Terdapat tiga forum internasional dimana China berperan aktif menyatakan misinya dalam *cyberspace*. Pertama adalah *World Internet Conference*, sebuah konferensi tahunan yang diprakarsai oleh China dan diadakan pertama kalinya pada tahun 2014. Dalam WIC, China menggaungkan *cyber sovereignty* dan perhatian China terhadap ekonomi internet. Sebagai wujud implementasi dari WIC, dibentuk

[134] Ibid.

sebuah komite yang berfungsi untuk menerapkan prinsip *cyber sovereignty* dalam *cyberspace* secara internasional, dan juga sebagai komite yang menjadi dewan penasihat bagi CAC.[135] Pemerintah China juga menggunakan kesempatan tersebut untuk melakukan pendekatan multi-stakeholder dengan turut mengundang pemimpin perusahaan teknologi dunia.[136]

Forum internasional kedua adalah SCO atau *Shanghai Cooperation Organisation.* SCO adalah sebuah organisasi internasional yang diprakarsai oleh China dan lima negara lainnya yaitu Rusia, Kyrgyzstan, Kazakhstan, Tajikistan, dan Uzbekistan. India dan Pakistan kemudian bergabung sebagai anggota pada tahun 2017.[137] Di dalam SCO, pendekatan yang diambil China adalah untuk memberantas terorisme melalui *cyberspace*. Agenda utama SCO adalah memperluas inisiatif ekonomi dan menghadapi ancaman keamanan non tradisional, dengan fokusnya terletak pada tiga poin yaitu terorisme, separatis, dan ekstrimis.[138]

Forum ketiga adalah *United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications*, sebuah kelompok kerja sebagai perwakilan pemerintah dalam ranah *cyberspace.* 15 negara ditunjuk oleh majelis umum PBB untuk menelaah permasalahan terkait keamanan informasi internasional.[139] Pada awalnya, pembahasan mengenai keamanan

---

[135] Segal, Op.Cit., p. 9.
[136] Josh Horwitz, 'Tim Cook and Sundar Pichai's surprise remarks at China's "open internet" conference', Quartz, <https://qz.com/1145637/2017-world-internet-conference-tim-cook-and-sundar-pichais-surprise-remarks/> [accessed 25 July 2018].
[137] Shanghai Cooperation Organization, *The Shanghai Cooperation Organisation*, 2017, <http://eng.sectsco.org/about_sco/> [accessed 30 February 2018].
[138] Segal, Op.Cit., p. 10
[139] Ke 15 negara UN GGE pada saat itu adalah Belarus, Brazil, China, France, Germany, India, Jordan, Malaysia, Mali, Mexico, the Republic of Korea, the Russian Federation, South Africa, the United Kingdom of Great Britain and Northern Ireland and the United States of America.

informasi didiskusikan dalam Komite Komite Pertama Majelis Umum PBB di bidang perlucutan senjata. Tahun 1998, Majelis Umum PBB menerima draft resolusi mengenai perkembangan teknologi informasi dan komunikasi dalam konteks keamanan internasional yang diserahkan oleh Rusia.[140] Sejak saat itu, anggota lainnya turut menyumbang pemikiran terhadap keamanan informasi hingga dibentuklah UN GGE pada tahun 2004.

UN GGE kemudian berhasil mencapai kesepakatan mengenai hukum internasional dalam *cyberspace.* Keputusan PBB disepakati sebagai hukum yang berlaku berdasarkan laporan UN GGE tahun 2013, dimana kedaulatan sebagai prinsip dasar hukum internasional dan yurisdiksi negara terkait penggunaan teknologi informasi.[141] China adalah salah satu negara yang menyepakati hal tersebut. Sedangkan dalam forum UN GGE tahun 2015, China bersama dengan Rusia kembali memperjuangkan kedaulatan internet. Dalam laporan akhir UN GGE, makna kedaulatan kedaulatan diperluas dalam konteks hukum internasional dan juga menambahkan prinsip non intervensi.[142]

4.5 Permasalahan Isu *cyber* yang dihadapi China dengan Amerika Serikat

Hubungan bilateral China dan AS diwarnai dengan ketegangan, konflik, dan kecurigaan terhadap satu sama lain. Keduanya bersaing untuk membawa pengaruh

[140] Segal, Op.Cit., p. 5.
[141] United Nations, Group of Governmental Experts, A/68/98. 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, June 24, 2013' < http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=E > [accessed 5 July 2018].
[142] United Nations, A/70/172. 'Developments in the Field of Information and Telecommunications in the Context of International Security, July 22, 2015' <http://undocs.org/A/70/172> [accessed 5 July 2018].

sebagai penjaga stabilitas kawasan, terutama di wilayah Asia, terutama sejak dikeluarkannya kebijakan '*pivot to Asia'* oleh rezim Obama. Rivalritas tersebut membawa ketegangan yang terjadi pada beberapa isu Strategis dalam hubungan bilateral China-AS diantaranya adalah isu *cybersecurity*.[143] China dan AS sama-sama menganggap bahwa aktivitas *cyber* yang dilakukan oleh satu sama lain merupakan ancaman bagi keamanan nasional masing-masing.

Permasalahan dalam isu *cyber* antara China dan AS berasal dari perbedaan pandangan dalam *cyberspace.* China menolak pandangan AS terkait kebebasan berinternet yang dapat membahayakan keamanan nasional China.[144] China menegaskan pada prinspinya yaitu kedaulatan internet sebagai dasar dari *cybersecurity.* Kebebasan internet dianggap China sebagai upaya AS untuk menghegemoni dan mengeksploitasi *cyberspace*. China mengkhawatirkan AS menggunakan teknologi *cyber* untuk mengembangkan kemampuan senjata *cyber* untuk melemahkan bahkan menjatuhkan negara yang tidak sejalan dengan AS. China berupaya untuk mencegah celah intervensi AS dalam urusan *cyber.*[145]

Prinsip kebebasan berinternet merupakan implementasi dari Hak Asasi Manusia yang merupakan nilai yang berasal dari barat.[146] China kemudian meningkatkan upaya untuk meningkatkan perannya secara internasional untuk membentuk prinsip dan nilai kedaulatan internet. Upaya tersebut dilakukan secara

[143] Chen Dingding, 'Shaping the future of Sino-American Relations Power Shift and Strategic Rivalry', in Mingjiang Li & Kalyan M. Kemburi (Ed.), *New Dynamics in US–China Relations* (Routledge, 2015), p. 56.
[144] McKune, Op.cit., pp. 265-266.
[145] Michael D. Swaine, 'Chinese Views of Cybersecurity in Foreign Relations,' *China Leadership Monitor,* No. 42, (2013), p. 11.
[146] McKune, Loc.cit.

bilateral maupun multilateral melalui *cyberdiplomacy,* yang salah satunya adalah dengan AS.

4.5.1 Permasalahan *cyber espionage* China dan Amerika Serikat

Aktivitas *cyber* yang dilakukan China telah lama menjadi perhatian AS. China telah dikenal sebagai pencuri data dalam sistem keamanan informasi AS, terutama sejak China berhasil mengumpulkan data militer AS menggunakan *Titan Rain* pada tahun 2003, dan aktivitas spionase melalui operasi *Shady RAT* tahun 2007.[147] Kasus lainnya menimpa sektor swasta pada tahun 2009. Google menuntut China dalam kasus peretasan dan kebocoran data, yang berakhir dengan hengkangnya mesin pencarian tersebut dari wilayah China. Perusahaan seperti Apple, Twitter, Facebook, The New York Times, The Wall Street Journal, dan the Washington Post, juga merupakan target serangan dari peretas China.[148] Hal ini menunjukkan bahwa sentimen yang ditujukan terhadap China tidak hanya berasal dari pemerintah AS, tetapi juga perusahaan yang merasa dirugikan oleh aktivitas peretas China.

Perlu diingat bahwa yang menjadi perhatian utama AS mengenai aktivitas *cyber* China adalah mengenai aktivitas spionase siber. Pemerintah China dituding melakukan EMCE atau *Economic Motive Cyber Espionage* dengan perkiraan total

[147] *Titan Rain* dan *Shady RAT* adalah kode yang diberikan oleh FBI untuk menyebut serangan *cyber* yang diduga berasal dari China dan memiliki keterkaitan dengan PLA. *Titan Rain* menyerang Departemen Pertahanan AS pada tahun 2003, sedangkan *Shady RAT* adalah operasi terhadap pemerintah dan perusahaan AS, diantaranya adalah perusahaan IT.

[148] Lee JA, 'The Sino-US Digital Relationship and International *Cyber* Security', in Lemieux F. (eds), *Current and Emerging Trends in Cyber Operations*. Palgrave Macmillan's Studies in *Cyber*crime and *Cyber*security, (Palgrave Macmillan: London, 2015), p. 87.

kerugian finansial yang dialami AS sebanyak $338 miliar per tahun.[149] Tudingan tersebut turut didukung oleh laporan yang berasal dari sebuah lembaga penelitian *cybersecurity* AS, 'Mandiant'. Laporan tersebut mengungkapkan keberadaan kelompok peretas China bernama Unit 61398 yang diduga berada di bawah komando langsung PLA.[150] Kelompok tersebut dianggap sebagai pelaku utama pencurian data yang menyebabkan kerugian bagi perusahaan maupun pemerintah AS.

Meskipun berulang kali dianggap sebagai pelaku spionase siber, China mengelak dengan konsisten segala tuduhan EMCE, seperti yang disampaikan oleh juru bicara menteri luar negeri China, Liu Weimin:

> "*The Chinese Government always opposes and strictly prohibits any illegal criminal activity by hackers. The Chinese law stipulates unequivocally that those who commit cyber crimes should undertake criminal liability in accordance with the Criminal Law of the People's Republic of China*."[151]

Pemerintah China berupaya memberantas aktivitas illegal yang dilakukan oleh peretas. Selain itu, hukum secara tegas berlaku bagi siapa saja pelaku kejahatan *cyber*, sesuai dengan hukum pidana yang berlaku. Selain itu, China juga menganggap bahwa tuduhan yang diberikan merupakan tuduhan yang tidak

---

[149] *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology*, Testimony of Larry M. Wortzel before the House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations, 2013, <http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf> [accessed 24 July 2018].

[150] Fire eye, *APT1 Exposing One of China's Cyber Espionage Units* <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> [accessed 24 July 2018].

[151] Embassy of the People's Republic of China in the United States, *Foreign Ministry Spokesperson Liu Weimin's Regular Press Conference on December 12, 2011*, 2011, <http://www.china-embassy.org/eng/fyrth/t887523.htm> [accessed 26 July 2018].

berdasar dan mengada-ada.[152] Hal tersebut dikarenakan oleh tuduhan AS hanya berdasarkan pada lokasi asal serangan yang diduga berasal dari salah satu markas divisi PLA, dimana hal tersebut tidak cukup membuktikan pelaku serangan *cyber* yang sesungguhnya.

Pernyataan lain yang ditegaskan sebagai bentuk respon China terhadap tuduhan AS adalah bahwasanya China sendiri merupakan korban dari spionase siber. Dalam setiap kesempatan, respon tersebut juga ditekankan kepada publik secara berulang. "*China is a victim of cyber attacks*"[153], dinyatakan secara jelas oleh Yang Yujun, seorang perwakilan dari Menteri Pertahanan China pada tahun 2012, dan ditegaskan kembali oleh juru bicara menteri luar negeri China, Hua Chunying dalam konferensi persnya tahun 2013.[154] Bagi China, tuduhan yang dilakukan AS pada dasarnya adalah sebagai alasan untuk menggunakan kemampuan *cyber* nya kepada China, dan membatasi perkembangan China di bidang teknologi.[155]

Berbeda dengan AS, China tidak berupaya memojokkan AS sebagai biang dari serangan *cyber* dengan mengatakan bahwa AS merupakan pelaku utama kepada publik. China hanya menegaskan bahwa China sendiri merupakan korban

---

[152] China Central Television, *China: Hacking allegations "groundless"*, 2013, <http://english.cntv.cn/program/newshour/20130220/104023.shtml> [accessed 14 December 2017].

[153]Xinhua, *China is victim of cyber attacks: spokesman*, 2012, <http://www.chinadaily.com.cn/china///2012-03/29/content_14946469.htm> [accessed 14 July 2018].

[154]Embassy of the People's Republic of China in the United States of America, *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 13,* 2013 < http://www.china-embassy.org/eng/fyrth/t1050375.htm>, & Embassy of the People's Republic of China in the United States of America, *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 28,* 2013 <https://www.fmprc.gov.cn/ce/cebn/eng/fyrth/t1054303.htm> [accessed 14 July 2018].

[155] China Military Online, *MND website and China Military Online attacked by overseas hackers 144,000-odd times per month*, 2013, <http://en.people.cn/90786/8151567.html> [accessed 17 July 2018].

dari serangan sembari menjelaskan bahwa serangan yang berasal dari AS mendominasi kasus peretasan yang terjadi di China.[156] Dijelaskan oleh Hong Lei, juru bicara menteri luar negeri China, pada tahun 2012 sebanyak 73.000 alamat IP asing mengontrol 14 juta computer yang berada di China, dan 32.000 alamat IP asing mengontrol 38.000 situs milik China secara jarak jauh.[157] Data tersebut selaras dengan penjelasan Menteri Pertahanan China — yang pada saat itu juga menjelaskan bahwa PLA tidak pernah mendukung adanya serangan *cyber* terhadap AS — bahwa di tahun yang sama, China mengalami serangan *cyber* yang berasal dari pihak asing sebanyak 144.000 kali per bulannya. [158]

Kegeraman China semakin diperkuat dengan adanya pembeberan aktivitas intelijen AS. Pada bulan Juni tahun 2013, terjadi Edward Snowden membeberkan aktivitas spionase yang dilakukan oleh NSA yang pada akhirnya meningkatkan skeptisme China dalam *cybersecurity* China-AS. Dalam pengakuannya, Edward Snowden menjelaskan bahwa NSA melakukan serangan *cyber* terhadap berbagai negara, diantaranya adalah China, Rusia, Iran, dan Korea Utara. Dua target utama spionase yang dilakukan NSA adalah perusahaan telepon genggam, dan sistem komputer Universitas China Hong Kong (CUHK). NSA mengumulkan data masyarakat China melalui pesan teks melalui jalur belakang untuk menyadap *sim card* yang terdapat dalam telepon genggam.[159] Pada saat ini, China masih

[156] Xinhua, 'Attacks originating from U.S. rank first among overseas hackings in China: FM,', *Global Times*, 2013 < http://www.globaltimes.cn/content/762961.shtml > [accessed 17 July 2018].
[157] Ibid.
[158] China Military Online, Loc.Cit.
[159] Lana Lam & Stephen Chen, 'US spies on Chinese mobile phone companies, steals SMS data: Edward Snowden', *South China Morning Post*, 2013, <https://www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden> [accessed 27 November 2017].

menggunakan teknologi AS dalam komponen teknologinya, sehingga menjadi celah keamanan yang terbukti dimanfaatkan oleh pihak asing seperti pemerintah AS. Sedangkan CUHK adalah salah satu pusat pendidikan mengenai pengembangan teknologi di China. Bahkan, melalui CUHK, pemerintah AS dapat mengambil data masyarakat China yang terdaftar dalam jaringan sistem pendidikan.[160]

Pembeberan aktivitas intelijen yang dilakukan oleh NSA membuktikan AS sebagai pelaku spionase siber terhadap China. AS melegitimasikan spionase yang dilakukan NSA adalah untuk kepentingan keamanan nasional, dimana pemerintah tidak menggunakan data yang dikumpulkannya kecuali untuk kebutuhan keamanan.[161] Berbeda dari EMCE, dimana pemerintah China dianggap berupaya mengambil keuntungan dari aktivitas ilegal tersebut. Dengan adanya pembeberan Snowden, tanggapan China terhadap pernyataan AS menjadi lebih sentimen. China menganggap AS melakukan standar ganda. China kemudian merespon AS dengan mengatakan bahwa AS tidak konsisten terhadap berbagai tuduhan yang diajukan kepada China, dimana AS sendiri merupakan pelaku dari spionase siber.[162]

Meskipun banyak terjadi hal-hal tidak terduga, tahun 2013 menjadi tahun yang mengawali perkembangan isu *cybersecurity* dalam hubungan AS-China. Apabila penelitian Mandiant dan pembeberan Edward Snowden meningkatkan skeptisme satu sama lain, Sunnylands Summit menjadi awal mula kerjasama dalam ranah *cyber*.[163] Kedua kepala negara tersebut bertemu untuk pertama kalinya

[160] Ibid.
[161] Ibid.
[162] Swaine, loc.cit., p. 42.
[163] Harold, Libicki, & Cevallos, Loc cit, hal. 9.

terhitung sejak presiden Xi Jinping menjadi pemimpin negara RRC. Kerjasama *cybersecurity* telah mendapatkan dukungan dari pihak negara China sejak lama.

Pada saat pertemuan Sunnyland Summit, *cybersecurity* menjadi topik hangat pembicaraan presiden Obama dan presiden Xi. Dalam pertemuan tersebut, terdapat beberapa hal yang ditekankan oleh China mengenai permasalahan *cybersecurity* dan hubungannya dengan AS:

" China is also a victim of cyber attack and firmly supports cyber security. On the issue of cyber security, China and America face common challenges. Instead of being a source of mutual suspicion and friction between China and America, cyber security should be a new highlight in the bilateral cooperation."[164]

China kemudian memberikan penekanan kembali bahwa China merupakan korban dari serangan *cyber*, setelah berulang kali menyatakannya dalam berbagai kesempatan yang lain. Dalam hubungannya dengan AS, China memahami tantangan yang diberikan dalam *cyberspace* dapat memunculkan rasa saling tidak percaya dan perselisihan terhadap satu sama lain. Tetapi hal tersebut tidak seharusnya menjadi menjadi sumber ketegangan kedua belah pihak. China mengatakan bahwa kerjasama justru menjadi hal yang dibutuhkan oleh keduanya.

Pada tahun 2014, pembicaraan mengenai isu *cybersecurity* terhenti dikarenakan keputusan AS untuk mendakwa 5 orang personil militer China yang diduga terhubung dengan PLA yaitu Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zheyu, dan Gu Chunhui. Para terdakwa diduga merupakan bagian dari PLA unit

[164] Ministry of Foreign Affairs, the People's Republic of China, *Yang Jiechi's Remarks on the Results of the Presidential Meeting between Xi Jinping and Obama at the Annenberg Estate*, 2013 <https://www.fmprc.gov.cn/mfa_eng/topics_665678/xjpttcrmux_665688/t1049263.shtml> [accessed 28 July 2018].

61398.[165] Dakwaan itu adalah tuduhan peretasan kriminal pertama yang dilakukan AS terhadap warga negara asing. China merespon kasus dakwaan dengan memberikan penegasan bahwa China merupakan korban dari serangan *cyber* yang dilakukan oleh AS, dan China juga membantah keterlibatannya dalam aktivitas spionase dalam bentuk apapun terhadap AS. Dakwaan yang ditujukan kepada warga negara China menunjukkan ketidaksesuaian antara perkataan dan sikap dari pemerintah AS. China kemudian menunda dialog dan kerjasama terkait isu spionase siber yang dilakukan bersama AS dalam *China-US Working Group* sebelum tuntutan tersebut dicabut.[166]

Kesepakatan terkait aktivitas spionase siber pada akhirnya mencapai konsensus pada bulan September tahun 2015. Kesepakatan tersebut menandai dimulainya kerjasama antara AS dan China dalam menghadapi ancaman *cyber*. Hal ini menjadi sebuah kemajuan dalam isu *cybersecurity* yang menjadi sumber ketegangan hubungan bilateral China-AS dalam beberapa tahun belakangan. Terlebih lagi, Beberapa sumber mengatakan bahwa terjadi penurunan tingkat aktivitas spionase siber oleh China setelah tercapainya kerjasama *cybersecurity* antara China dan AS.[167] Setiap pihak pun mulai mengantisipasi terhadap perkembangan isu *cybersecurity* kedepannya.

---

[165] Department of Justice, *US. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, 2014 <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-*cyber*-espionage-against-us-corporations-and-labor> [accessed 29 July 2018].

[166] Ministry of Foreign Affairs, the People's Republic of China, *China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel*, 2014 <http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1157487.shtml> [accessed 30 July 2018].

[167] FireEye, "Redline Drawn: China Recalculates its use of Cyber Espionage" (special report, FireEye, June 2016), <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-chinaespionage.pdf.> > [accessed 30 July 2018].

BAB V

PEMBAHASAN

5.1 Aktivitas Diplomatik China dan AS dalam Isu *Cybersecurity*

Aktivitas diplomasi yang dilakukan oleh China secara bilateral dengan AS adalah melalui dialog dan pertemuan bilateral antara perwakilan kedua negara. China melakukan *cyberdiplomacy* melalui beberapa jalur diplomasi , yaitu track 1 dan track 1.5. Track 1 adalah ketika representasi negara merupakan perwakilan pemerintah. Sedangkan track 1.5 adalah ketika representasi yang hadir adalah aktor non negara seperti pemimpin perusahaan dan perwakilan organisasi, tetapi turut melibatkan perwakilan pemerintah negara tersebut.[168]

5.1.1 *US-China Cybersecurity Dialogue*

Isu *cybersecurity* telah menjadi agenda dalam forum bilateral China dan AS sejak tahun 2009 dengan nama "*U.S.-China Cyber Security Dialogue".*[169] Pertemuan ini dikatakan sebagai jalur diplomasi track 1.5. Dialog ini memang tidak diwakili oleh perwakilan pemerintah seluruhnya, sehingga perspektif yang ada dalam dialog ini tidak dapat seluruhnya mewakili pemerintah China. Meskipun begitu, analisis mengenai dialog ini merupakan hal yang penting. Informasi didalamnya dapat dikatakan cukup relevan, dikarenakan oleh sumber informasi

[168] B. R. Gerridge, *Diplomacy: Theory and Practice* , Fourth Edition, (Palgrave : Hampshire : 2009), p. 238.
[169] Scott Warren Harold, Martin C. Libicki, Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace*, p. 49-51, <http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf> [accessed 27 September 2018].

merupakan hasil pemikiran antara perwakilan pemerintah, akademisi maupun *think tanks* yang secara konsisten menjadi pengamat di bidang isu *cybersecurity.*[170] Melalui dialog ini, terdapat informasi mengenai perkembangan permasalahan dalam hubungan *cybersecurity* China dan AS mulai dari tahun 2009 hingga tahun 2017. CICIR dan CSIS telah melakukan dialog sebanyak sebelas kali pertemuan. Tetapi, dialog ini bersifat rahasia sehingga tidak banyak informasi yang ditampilkan bahkan dalam situs CSIS maupun situs resmi CICIR.

Sesuai dengan tujuannya, dialog ini merupakan langkah awal setiap pihak untuk membangun kepercayaan terhadap satu sama lain. Tujuan diadakannya *U.S.-China Cyber Security Dialogue* adalah menumbuhkan kepercayaan terhadap satu sama lain dalam permasalahan *cybersecurity*. Pertemuan ini menjadi jalur komunikasi reguler untuk mengidentifikasi area yang berpotensi untuk mengurangi mispersepsi dan meningkatkan transparansi, mencapai kerjasama *cybersecurity* dan mencapai kesepakatan terhadap norma dan aturan yang berlaku dalam *cyberspace*.[171] Tidak hanya itu, dialog ini juga bertujuan untuk mengidentifikasi potensi kerjasama dalam hubungan China dan AS, termasuk juga upaya *Confidence Building Measure.* Meskipun belum sampai pada tahap CBM, tetapi topik yang dibahas dalam diskusi *U.S.-China Cyber Security Dialogue* dinilai telah mendekati proses persiapan dalam melakukan CBM.[172] Keduanya masih berada dalam tahap

---

[170] Juan Manuel De La Torre Davila, 'Cybersecurity and United States-China Relations: A Theoritical Perspective', (International Master's Program in International Studies National Chengchi University, 2018), pp. 49-50.

[171] China Institute of Contemporary International Relations (CICIR) and Center for Strategic and International Studies (CSIS), *Bilateral Discussions on Cooperation in Cybersecurity*, 2012, <http:// csis.org/files/attachments/120615_JointStatement_CICIR.pdf> [accessed 27 June 2018].

[172] Katharina Ziolkowski, 'Confidence Building Measures for Cyberspace', in K. Ziolkowski (Ed.), *Peacetime regime for state activities in cyberspace: International law, international relations and diplomacy* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2013), p. 551.

memahami dan menata perilaku yang dianggap sebagai ofensif atau memicu perang dalam *cyberspace*, dan menyesuaikannya dengan hukum maupun norma yang belaku dalam *cyberspace*.

5.1.2 *U.S.-China Strategic and Economic Dialogue* (S&ED)

U.S.-China Strategic and Economic Dialogue (S&ED) merupakan dialog bilateral antara China dan AS untuk membahas isu strategis dalam hubungan bilateral kedua negara. Isu yang dibahas sangat beragam, terutama isu-isu di bidang keamanan dan ekonomi dalam hubungan bilateral kedua negara. Dalam bidang keamanan, S&ED memiliki beberapa forum dialog yang dibawahinya, salah satunya adalah *Strategic Security Dialogue* (SSD). Tujuan diadakannya dialog S&ED adalah untuk membangun kepercayaan antara kedua negara dan membangun kerjasama dalam model hubungan baru antara China dan AS. [173] Sebelum adanya kerangka dialog tingkat tinggi yang secara khusus membahas isu-isu *cyber*, S&ED menjadi sarana bagi China dan AS untuk mendiskusikan perihal permasalahan *cyberspace* dalam hubungan bilateral kedua negara.

Setelah presiden Xi dan presiden Obama bertemu pada Sunnyland Summit di tahun 2013, keduanya sepakat untuk membawa isu *cybersecurity* dalam sebuah forum bilateral.[174] *Cybersecurity* kemudian menjadi agenda dalam pertemuan bilateral China dan AS dalam S&ED kelima melalui *U.S.-China Cyber Working*

[173] Embassy of the People's Republic of China in the United States of America, *U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track*, 2013, <http://www.china-embassy.org/eng/zmgxss/t1058593.htm> [accessed 29 June 2018].
[174] Office of the Press Secretary, *Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting*, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china- > [accessed 29 June 2018].

Group atau CWG. [175] CWG adalah sebuah kelompok kerja atau *working group* yang dibentuk dibawah kerangka S&ED. Pembentukan CWG telah ditentukan sejak April 2013, tetapi pertemuan pertama baru dilakukan pada bulan Juli tahun 2013, tepat pada hari pertama pertemuan S&ED kelima. CWG dibentuk sebagai perwujudan keresahan China dan AS dalam permasalahan spionase siber seperti yang menjadi pembahasan dalam pertemuan antara kedua pemimpin negara.

Pembentukan CWG memperlihatkan adanya peningkatan terhadap pentingnya isu *cybersecurity* dalam hubungan bilateral China dan AS. CWG melibatkan representasi langsung dari pemerintah dengan agenda diplomatik tertentu. Terlihat pula adanya upaya pembentukan kerangka kerjasama secara teknis untuk meningkatkan *cybersecurity.* Meskipun belum mencapai adanya kesepakatan yang terstruktur, China berupaya untuk meningkatkan kepercayaannya dalam hubungan *cybersecurity* dengan AS. Di dalam CWG, Keduanya sepakat untuk tidak hanya melakukan peningkatan tenaga ahli di bidang *cyberspace*, tetapi juga membangun kerangka kerjasama dalam bidang penegakan hukum.[176] Terdapat beberapa hasil dialog yang mengarah pada suatu kerjasama yang positif. Bahkan, dalam pertemuan S&ED kedelapan yang dilaksanakan pada tahun 2016, China dan AS sepakat untuk membentuk dialog tingkat tinggi yang berfokus pada isu *cybercrime* dan isu-isu terkait lainnya.[177]

---

[175] Embassy of the People's Republic of China in the Republic of Kenya, *The Third China-U.S. Strategic Security Dialogue Held in Washington, D.C.*, 2013, <http://ke.china-embassy.org/eng/zgyw/t1058060.htm> [accessed 29 June 2018].
[176] Embassy of the People's Republic of China in the United States of America, Loc.cit.
[177] Office of the Spokesperson, *U.S.-China Strategic & Economic Dialogue Outcomes of the Strategic Track*, 2016, <https://2009-2017.state.gov/r/pa/prs/ps/2016/06/258146.htm> [accessed 29 June 2018].

Pertemuan ini memberikan sinyal keduanya bahwa hubungan *cybersecurity* China dan AS berjalan ke arah yang lebih baik.[178] Akan tetapi, sangat disayangkan bahwa forum bilateral CWG yang baru sampai pada pertemuan pertama tidak mendapatkan kelanjutan. Pada tahun 2014, China menunda CWG sebagai responnya terhadap pendakwaan terhadap warga negara China oleh AS. Hal ini terlihat pada pertemuan S&ED keenam yang berlangsung pada Juli 2014. Pertemuan tersebut tidak mengandung pembahasan mengenai isu *cybersecurity* seperti yang telah dibahas sebelumnya.

5.1.3 Kunjungan Kenegaraan Presiden Xi Jinping ke Amerika Serikat

Seminggu sebelum pertemuan antara presiden Xi Jinping dan Barack Obama, Meng Jianzhu diutus untuk melakukan kunjungan ke AS. Kunjungan Meng ke AS bertujuan untuk menyampaikan mengenai posisi China dalam isu *cyber* yang dialami kedua negara. Ia menyampaikan bahwa China akan memerangi segala bentuk spionase spionase siber dan akan dengan tegas menghukum para pelakunya.[179] Seminggu kemudian, presiden Xi secara resmi melakukan kunjungan ke Washington yang pada akhirnya melahirkan kesepakatan bilateral *'US-China Cyber Agreement'.*

[178] Yang Qingchuan, 'Commentary: China-U.S. dialogue to transcend talks of cyber security', *China Central Television*, 2013, http://english.cntv.cn/20130710/103009.shtml> [accessed 30 June 2018].
[179] The Diplomat, *A delegation of Chinese officials visited the U.S. for talks on cybersecurity issues*, 2015, <https://thediplomat.com/2015/09/us-china-hold-cyber-talks-before-xis-visit/> [accessed 30 june 2018].

Poin-poin kesepakatan yang dicapai oleh presiden Xi Jinping dengan presiden Barack Obama pada saat kunjungannya ke Washington adalah sebagai berikut[180]:

- *Both sides agree* ***to cooperate,*** *in a manner consistent with their respective national laws and relevant international obligations, with requests* ***to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity*** *emanating from their territory.*

- *Both sides also agree* ***to provide updates on the status and results of those investigation to the other side***.

- *China and the United States agree* ***that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors***.

- *Both sides are committed to making common effort to further* ***identify and promote appropriate norms of state behavior*** *in cyberspace within the international community.*

- *The two sides also agree* ***to create a senior experts group*** *for further discussions on cybersecurity.*

- *China and the United States agree* ***to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues***. *This mechanism will be used* ***to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side.***

- *Both sides agree* ***to establish a hotline*** *for the escalation of issues that may arise in the course of responding to such requests.*

- *Both sides agree that the first meeting of this dialogue will be held by the end of 2015, and* ***will occur twice per year*** *thereafter.*

[180] The Ministry of Foreign Affairs of the People's Republic of China, *Full Text: Outcome list of President Xi Jinping's state visit to the United States*, 2015, <https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1300771.shtml> [accessed 30 June 2018].

Pertama, poin diatas menjelaskan bahwa keduanya sepakat untuk bekerjasama dalam menghadapi segala bentuk *cybercrime* melalui hukum internasional yang ada maupun hukum nasional masing-masing pihak, termasuk di dalamnya memenuhi permintaan investigasi dan pemenuhan bukti elektronik, dan pencegahan potensi ancaman yang berasal dari teritori masing-masing. Pada poin ini, terlihat bahwa keduanya saling menghormati hukum yang berlaku pada masing-masing negara, tanpa adanya paksaan untuk membentuk suatu sstem hukum baru dalam kerjasama tersebut.[181]

Poin selanjutnya menjelaskan kesepakatan terhadap perlawanan terhadap *cybercrime* dilakukan dengan bekerjasama dalam berbagi informasi dan hasil investigasi kepada satu sama lain. Lalu, tidak melakukan ataupun mendukung pencurian data dan juga kekayaan intelektual, termasuk juga rahasia dagang maupun rahasia informasi bisnis untuk kepentingan komersial dengan tujuan menyediakan keunggulan kompetitif bagi perusahaan. Kedua belah pihak berkomitmen untuk membentuk dan mengembangkan norma perilaku *cyberspace* di dalam komunitas internasional, begitu juga dengan bekerjasama secara internasional untuk tujuan yang sama.

Terakhir, keduanya bersepakat untuk membentuk mekanisme dialog tingkat tinggi dengan fokus memberantas *cybercrime* dan isu-isu terkait. Upaya yang akan dilakukan antara lain membangun *cyber hot-line*[182] dan melakukan pertemuan dua

[181] Juan Manuel De La Torre Davila, Op.cit., p. 64.
[182] ***Cyber hot-line*** adalah saluran telepon khusus untuk tujuan komunikasi permasalahan *cyberspace* yang langsung menghubungkan antara dua kepala negara. China dan AS membangun jaringan komunikasi yang dapat saling mengawasi keduanya dalam menerapkan norma *cyberspace* sesuai dengan keputusan UN GGE. Dikutip dari Duncan B. Hollis, *China and the US Strategic*

kali dalam satu tahun untuk meninjau kualitas kemampuan kedua belah pihak dalam menanggapi kasus *cybercrime* dan kemampuan dalam memberikan bantuan informasi terkait aktivitas *cyber* berbahaya. Poin tersebut menggambarkan bahwa untuk pertama kalinya China dan AS membentuk sebuah dialog tingkat tinggi terkait permasalahan *cyber*, dimana hal tersebut merupakan salah satu poin rekomendasi yang telah dijelaskan dalam *U.S.-China cybersecurity dialogue*.[183]

Melalui kerjasama *cybersecurity*, kedua negara sepakat untuk melakukan kerjasama untuk mengatasi *cybercrime*, asistensi investigasi, dan upaya pembentukan norma internasional bersama, yaitu norma perilaku spionase siber dengan tujuan komersial. Melalui kerjasama tersebut, maka spionase siber telah secara resmi dianggap sebagai perilaku illegal dalam *cyberspace*. Mekanisme tersebut juga didukung dengan tujuan meningkatkan kualitas respon terhadap permintaan asistensi informasi mengenai aktivitas *cyber* berbahaya. Sehingga, di dalam mekanisme yang akan dibangun tidak hanya berdiskusi mengenai masalah teknis *cybersecurity* tetapi juga mengembangkan kerjasama ini untuk menjadi lebih terstruktur kedepannya.

5.1.4 *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*

Sebagai bentuk implementasi dari *US-China Cyber Agreement* pada tahun 2015, China dan AS mengadakan *US-China High Level Joint Dialogue on Cybercrime and Related Issues*. Dialog ini adalah wajah baru dialog bilateral

Construction of Cybernorms: The Process Is the Product, Hoover Working Group on National Security, Technology, and Law, Aegis Paper Series No. 1704 (2017), p. 13.
[183]Juan Manuel De La Torre Davila, Op.cit., p. 66.

tingkat tinggi antara China dan AS dan merupakan salah satu saluran komunikasi keduanya untuk menyepakati area kerjasama *cybersecurity* yang sebelumnya mengalami penundaan pada tahun 2014. Sebelum berubah menjadi LECD, China dan AS telah bertemu dalam forum ini ketiga kalinya pada bulan Desember tahun 2018.[184]

Objektif utama dari dialog ini adalah untuk meninjau ketepatan waktu dan kualitas respon terhadap permintaan asistensi maupun informasi mengenai permasalahan *cybercrime* dan isu-isu Dialog ini juga bertujuan untuk mengembangkan kerjasama yang telah dicapai antara China dan AS, terutama mengenai isu *cybercrime.*[185] Pertemuan telah dilakukan sebanyak tiga kali, dimana setiap pertemuan menghasilkan perkembangan dalam isu terkait. Kerjasama yang terlihat disini antara lain adalah kerjasama dalam upaya menghadapi kasus *cybercrime*, bantuan permintaan asistensi, dan kerjasama di bidang penegakan hukum.

5.1.*5 U.S.-China Law Enforcement and Cybersecurity Dialogue* (LECD)

Pada tanggal 4 Oktober 2017, Cina dan Amerika Serikat mengadakan dialog tingkat tinggi dengan nama *U.S.-China Law Enforcement and Cybersecurity Dialogue* (LECD). LECD itu sendiri merupakan salah satu dialog empat pilar yang dihasilkan dari pertemuan presiden Xi dan presiden Trump pada bulan April

[184] The State Council The People's Republic of China, *China, US urge maintenance of bilateral dialogue mechanism to combat cybercrime*, 2016, <http://english.gov.cn/state_council/state_councilors/2016/12/08/content_281475510995959.htm> [accessed 3 July 2018].
[185] U.S. Department of Justice, *First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes*, 2015, <https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialoguecybercrime-and-related-issues-summary-outcomes-0> [accessed 3 July 2018].

sebelumnya di Mar A Lago. Dialog tersebut antara lain adalah; *Diplomatic and Security Dialogue, the Comprehensive Economic Dialogue, the Law Enforcement and Cybersecurity Dialogue,* dan *the Social and Cultural Issues Dialogue.*[186] Keempat dialog yang telah disebutkan sebelumnya kemudian menggantikan dialog S&ED yang telah berlangsung sejak tahun 2009 sampai dengan tahun 2016.

LECD merumuskan kerjasama yang akan dibangun yang berfokus pada 4 isu yaitu repatriasi, pemberantasan narkotika dan obat-obatan terlarang, perlakuan terhadap buron, *cybercrime* dan *cybersecurity*.[187] Diantara berbagai pokok pembahasan, *cybersecurity* adalah salah satu mekanisme yang berkembang melalui forum ini. Hal ini menandakan bahwa isu *cyber* telah menjadi perhatian utama dalam hubungan bilateral China dan AS bersama dengan isu-isu Strategis lainnya. Kerjasama *cybersecurity* telah terintegrasi melalui kerjasama dalam bidang penegakan hukum. Terlebih lagi, pembentukan kerangka LECD terjadi ketika AS telah memasuki babak baru dalam pemerintahannya. Hal tersebut turut memberikan tantangan baru bagi upaya *cyberdiplomacy* yang dilakukan oleh China. Tetapi, keberlanjutan dari dialog *cybersecurity* telah menunjukkan adanya konsistensi kedua belah pihak untuk menjaga hubungan *cybersecurity.*

5.2 Kepentingan Nasional China berdasarkan *International Strategy of Cooperation on Cyberspace*

Upaya China menghadapi peluang dan tantangan yang diberikan oleh *cyberspace* dilakukan berdasarkan Strategi *cyber* internasional China yang

[186] China Daily, *Summary of outcomes of First China-US Law Enforcement and Cybersecurity Dialogue,* 2017, <http://www.chinadaily.com.cn/world/2017-10/06/content_32924234.htm> [5 July 2018].
[187] Ibid.

dirumuskan dalam *International Strategy of Cooperation on Cyberspace.* Dokumen tersebut berisi penjelasan mengenai prinsip dasar dan posisi China dalam urusan *cyberspace* internasional. Prinsip tersebut kemudian dielaborasikan melalui Strategi dan rencana aksi dalam melakukan hubungan luar negeri terutama dalam bentuk kerjasama internasional.

Bagi China, terdapat empat prinsip dasar dalam *cyberspace* yaitu *peace, sovereignty, shared governance,* dan *shared benefit.*[188] Dasar dalam hubungan China dengan negara lainnya adalah dengan menjunjung tinggi prinsip perdamaian:

> *"The international community should observe the purposes and principles enshrined in the UN Charter in real earnest, particularly* ***non-use of force and peaceful settlement of disputes,*** *in order to ensure peace and security in cyberspace. . . . Countries should* ***reject the Cold War mentality, zero-sum game and double standards****, uphold peace* ***through cooperation*** *and seek one's own security through common security on the basis of full respect for other countries' security."*[189]

Prinsip perdamaian yang ditekankan oleh China berpegang teguh pada nilai-nilai yang ada dalam piagam PBB penyelesaian masalah secara damai dan bukan dengan adu kekuatan. China menekankan bahwa setiap negara seharusnya tidak lagi memiliki mental perang dingin, *zero sum game* dan standar ganda. Terlebih lagi, melalui prinsip perdamaian ini China mendorong kerjasama sebagai solusi atas penyelesaian masalah antar negara, bukan sebaliknya.

---

[188] Ministry of Foreign Affairs of the People's Republic of China, *International Strategy of Cooperation on Cyberspace*, 2017, <https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml > [accessed 5 July 2018].
[189] Ibid.

Prinsip selanjutnya adalah prinsip *sovereignty* atau kedaulatan. Bagi China, kedaulatan adalah dasar dari segala bentuk kebijakan dalam pemerintahannya.[190] Dokumen tersebut mengatakan bahwa

> *". . . **Countries should respect each other's right to choose their own path** of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. **No country should pursue cyber hegemony**, interfere in other countries' internal affairs, or engage in, condone or support cyber activities that undermine other countries' national security."*[191]

China meyakini bahwa kedaulatan adalah hak setiap negara, termasuk juga kedaulatan dalam *cyberspace.* Setiap negara dapat menentukan sendiri arah kebijakan internetnya, baik dari segi kebijakan publik maupun regulasi internet. Setiap negara juga memiliki hak yang sama untuk berpartisipasi dalam *cyberspace.* Selain itu, China menentang segala bentuk hegemoni *cyberspace* dan segala aktivitas yang dapat membahayakan keamanan negara lainnya dalam ranah *cyber.*

Poin yang terdapat dalam prinsip kerjasama maupun kedaulatan menyuarakan hal yang sama seperti pidato Xi Jinping dalam *World Internet Conference* tahun 2015. Pada saat itu, Xi Jinping memperkenalkan konsep yang dinamakan dengan *cyber sovereignty*, atau kedaulatan *cyber* sebagai norma dasar dalam hubungan antar negara.[192] Perlu diketahui bahwa, pemahaman mengenai

---

[190] Niels Nagelhus Schia and Lars Gjesvik, *China's cyber sovereignty*, The Norwegian Institute of International Affairs (2017), p. 1.
[191] Ministry of Foreign Affairs of the People's Republic of China, *International Strategy of Cooperation on Cyberspace*, Loc.cit.
[192] Ministry of Foreign Affairs of the People's Republic of China, *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference*, 2015, <http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml> [accessed 6 July 2018].

cyber sovereignty sebagai kepentingan nasional disini tidak melihat *cyber sovereignty* dalam konteks strategi militer di bidang *cyberspace,* tetapi melihat *cyber sovereignty* sebagai prinsip dasar pedoman perilaku *cyberspace* dalam konteks hubungan negara China melalui diplomasi.[193]

Prinsip ketiga dan keempat adalah *shared governance* dan *shared benefit.* Karena ranah *cyberspace* dapat diakses oleh entitas apapun, pengembangan *cyberspace* menjadi tanggung jawab bersama secara multilateral. Untuk itu, setiap negara berhak untuk memiliki andil dalam pembentukan norma *cyberspace* melalui peningkatan dialog dan mekanisme kerjasama. Selain itu, terlihat bahwa China berulang kali memberikan penekanan terhadap peran yang dimiliki PBB sebagai institusi yang berhak untuk menentukan norma dalam *cyber,* mengingat prinsip yang disebutkan oleh China sendiri juga mengacu pada prinsip yang terdapat dalam piagam PBB.

> *". . . **International cyberspace governance should follow a multilateral approach**. Countries should enhance communication, improve cyberspace-related dialogue and consultation mechanisms and jointly develop international cyber rules. **The United Nations should play a leading role** in coordinating positions of various parties and building international consensus."*[194]

Sedangkan *shared benefit* menjelaskan bahwa pengembangan *cyberspace* diharapkan dapat memberikan manfaat hingga ke lapisan masyarakat. Manfaat tersebut dapat dirasakan secara ekonomi melalui pertumbuhan ekonomi global dan

[193] Terdapat beberapa artikel yang menjelaskan *cyber sovereignty* adalah kedaulatan terhadap *cyberspace* dalam konteks militer. *White Paper* tahun 2015 menyebutkan *cyberspace* sebagai ranah komando utama. Lalu, *Cyberspace* dapat digunakan sebagai strategi militer oleh PLA untuk melindungi kedaulatan China.

[194] Ministry of Foreign Affairs of the People's Republic of China, *International Strategy of Cooperation on Cyberspace,* Loc.cit.

melalui pembangunan berkelanjutan. Oleh sebab itu, peningkatan kerjasama diperlukan untuk saling memberikan dukungan kekuatan terhadap satu sama lain.[195]

Segala prinsip dalam *cyberspace* yang dimiliki oleh China kemudian dirumuskan dalam tujuan strategis. Tujuan tersebut antara lain; untuk melindungi kedaulatan negara, mengembangkan kepentingan China dalam *cyberspace*, mengamankan arus informasi dalam internet, meningkatkan jaringan global, menjaga perdamaian, keamanan, dan stabilitas dalam *cyberspace*, membangun aturan internasional dalam *cyberspace*, mendorong pengembangan ekonomi global, dan meningkatkan pertukaran budaya dalam pengembangan internet.[196] Untuk mencapai tujuannya, tertulis dalam dokumen mengenai rencana aksi yang telah dicanangkan China. Pertama, China secara konsisten berpartisipasi aktif dalam proses pengembangan di bidang *cyber.* Kedua, China berusaha untuk meningkatkan hubungan bilateral dan regionalnya melalui dialog dan kerjasama. Lalu, China mendorong adanya upaya bersama untuk meningkatkan rasa percaya terhadap satu sama lain, dengan tujuan utama untuk menyusun sistem tata kelola internet global yang adil bagi setiap negara.[197]

5.2.1 Kepentingan Nasional *Cyberdiplomacy* China

Melalui *International Strategy of Cooperation on Cyberspace*, penelitian ini mencoba memberikan gambaran mengenai kepentingan dalam *cyberdiplomacy* yang dilakukan oleh China terhadap AS. Mula-mula, penelitian ini melihat prinsip

[195] Ibid.
[196] Ibid.
[197] Ibid.

dasar yang dimiliki oleh China dalam *cyberspace*. Prinsip tersebut menjadi dasar kebijakan yang diambil China dalam politik luar negerinya. Dua prinsip utama yang digunakan China dalam melakukan *cyberdiplomacy* dengan AS adalah prinsip perdamaian dan prinsip kedaulatan. Prinsip *shared governance* dan *shared benefit* bukan merupakan prinsip dominan, tetapi terlihat bahwa China mengupayakan kerjasama sebagai upaya pembentukan norma *cyberspace* melalui kerjasama internasional.

China melihat tuduhan AS yang ditujukan kepadanya sebagai upaya hegemoni AS dalam *cyberspace.* Dokumen yang dirilis gedung putih mengenai Strategi AS dalam cyberspace pada tahun 2011 dianggap sebagai upaya AS untuk menjadi hegemon dengan memiliterisasi *cyberspace,* dan sebagai bentuk dominasi AS di bidang teknologi.[198] Hal tersebut didukung oleh upaya AS menerapkan prinsip dasar kebebasan internet dan membentuk norma spionase *cyber*. China beranggapan bahwa kebebasan berinternet adalah cara yang digunakan AS untuk melakukan intervensi *cyberspace.*[199] China seringkali merespon tuduhan AS dengan menyebutkan AS sebagai negara bermental perang dingin[200] yang dan juga menerapkan standar ganda dalam membangun norma EMCE.[201]

---

[198] Adam Segal, 'Chinese Cyber Diplomacy in a New Era of Uncertainty', *Hoover Working Group on National security, Technology, and Law*, Aegis Paper Series No. 1703, (Stanford University, 2017), p. 4.

[199] Michael D. Swaine, 'Chinese Views of Cybersecurity in Foreign Relations,' *China Leadership Monitor,* No. 42, (2013), p. 42.

[200] Xinhua, 'Commentary: Pentagon's annual China military report exposes U.S. Cold War mentality', *People's Daily*, 2012, <http://en.people.cn/102774/7821676.html> [accessed 9 September 2018].

[201] Embassy of the People's Republic of China in the United States of America, *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 13,* 2013, < http://www.china-embassy.org/eng/fyrth/t1050375.htm> [accessed 14 September 2018].

Dalam upaya menyelesaikan perdebatan *cybersecurity* dengan AS, China memilih jalur damai melalui dialog bilateral. China bahkan mengambil keputusan untuk menyepakati kerjasama *cybersecurity* dengan AS. Upaya untuk menjaga perdamaian dalam hubungan *cybersecurity* antara China dan AS telah dilakukan sejak awal pertama dilakukannya dialog bilateral dengan tujuan untuk meningkatkan kepercayaan antara keduanya. Kerjasama tersebut juga mencerminkan bahwa China masih menghormati hubungan relasi China dan AS dalam *New Type of Major Power Relations.*

Seperti yang telah dijelaskan sebelumnya, dialog bilateral yang dilakukan oleh China dan AS mempertahankan hubungan *cybersecurity* keduanya agar tidak berkembang menjadi konflik yang lebih besar. Sebelum mencapai kerjasama pada tahun 2015, China tidak pernah menyetujui adanya pembentukan norma EMCE dalam *cyberspace.* Hal ini ditunjukkan China dengan penundaan *U.S.–China working group* pada tahun 2014.[202] Tetapi, dengan melakukan kerjasama *cybersecurity*, terjadi perubahan posisi yang diambil China terkait EMCE. Karena dengan menyepakati kerjasama tersebut, China turut serta berperan membangun norma EMCE sebagai norma *cyberspace.* Selain itu, melalui kerjasama tersebut China mempertegas posisinya dalam dunia internasional untuk menghadapi kejahatan *cyberspace.*[203]

Sedangkan prinsip kedaulatan adalah nilai yang dijunjung tinggi oleh pemerintah China. Dalam *cyberspace,* China memperjuangkan prinsip kedaulatan

[202] Roger Hurwitz, 'The State of Play: Norms and Security in Cyberspace', *American Foreign Policy Interests,* Vol. 36, No.5, (2014), p. 329.
[203] Swaine, Op. cit., p. 11.

yang dinamakan dengan *cyber sovereignty.* Dialog ini mengawali perjuangan China mengenai prinsip *cyber sovereignty* dalam dialog bilateralnya bersama dengan AS. *Cyber sovereignty* terus ditekankan sebagai prinsip dasar *cybersecurity*.[204] China secara konsistens menekankan nilai *cyber sovereignty* sebagai prinsip dasar politik luar negeri China dalam *cyberspace.* Hal tersebut menjadi upaya China dalam membangun norma internasional *cyberspace.*

5.2.2 *Cyber sovereignty*

Cyber sovereignty memiliki empat prinsip dasar utama.[205] Pertama adalah *independent,* yaitu setiap negara memiliki hak untuk membentuk kebijakannya sendiri terkait *cyberspace.* Kedua adalah *jurisdiction,* bahwa *cyberspace* memiliki kedaulatan yang bersifat territorial bagi negara. Hukum yang berlaku di dunia nyata juga berlaku dalam *cyberspace*, dikarenakan oleh jaringan internet juga dihubungkan dengan jaringan di dunia nyata. Akibatnya, sifat transnasional dalam internet tidak menghilangkan unsur kedaulatan negara.[206] Ketiga, setiap negara memiliki hak untuk turut andil dalam tata kelola internet global, dimana kedaulatan internet adalah prinsip dasar dalam menangani permasalahan *cyber* secara internasional.[207] Prinsip selanjutnya adalah *defense*, bahwa *cyberspace* digunakan negara sebagai sumber daya keamanan, begitu juga dengan kedaulatan untuk

---

[204] CICIR & CSIS, Loc.cit.
[205] Ministry of Foreign Affairs of the People's Republic of China, *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference,* 2015, <http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml> [accessed 6 July 2018].
[206] CICIR & CSIS, Loc.cit.
[207] Yi Shen, 'Cyber Sovereignty and the Governance of Global Cyberspace', *Chinese Political Science Review,* Vol.1, Issue 1, (2016), pp. 81–93, (p. 90).

mengatur masuknya informasi ke dalam wilayahnya sebagai bentuk pencegahan keamanan.

Cyber sovereignty adalah salah satu cara yang digunakan China untuk membangun tata kelola internet. Tujuan strategis yang ingin dicapai oleh China menggambarkan politik luar negeri asertifnya, begitu juga dalam hubungan *cybersecurity* dengan AS. China berupaya untuk secara aktif membangun tata kelola internet melalui melalui *cyber sovereignty.*[208] Hal ini didukung oleh artikel dalam jurnal *Quishi* yang menjelaskan bagaimana strategi Xi Jinping menaruh pentingnya *cybersecurity* China dengan tujuan menjadikan China sebagai negara dengan kekuatan *cyber.*[209] Salah satu caranya adalah penting bagi China untuk meningkatkan peran dalam pembentukan norma *cyberspace* internasional.

Cyber sovereignty mengandung model tata kelola internet yang berfokus pada peran negara sebagai aktor utama penentu kebijakan. China memperjuangkan adanya model tata kelola internet dimana semua negara dapat berpartisipasi bersama-sama untuk membangun aturan yang ada dalam *cyberspace,* yang dinamakan dengan model *multilateral.* Hal ini selaras dengan apa yang diajukan Xi Jinping melalui "*community of cyberspace destiny".* China menolak adanya dominasi tunggal dalam *cyberspace,* terutama dominasi AS sebagai negara yang memimpin kemajuan teknologi saat ini.[210]

---

[208]Nigel Inkster, *China's Cyber Power,* Adelphi Series, Vol. 55, No. 456, (2015), pp. 51-82 (p. 15).
[209] Cyberspace Administration of China Theoretical Studies Center Group, 'In-depth implementation of General Secretary Xi Jinping's network strategy of strengthening the country and solidly promoting network security and informationization', *Qiushi,* September 15 2017, <http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm> [accessed 18 September 2018].
[210] Binxing, Loc. Cit., p. 122-123.

Tata kelola internet multilateral merupakan sebuah konsep yang berlawanan dengan *multi-stakeholder*, yaitu pemberian hak yang sama kepada para *stakeholder* yang berperan dalam ranah *cyberspace*, seperti halnya individu maupun perusahaan. Dalam sudut pandang *multi-stakeholder*, tidak ada penekanan terhadap otoritas sentral dalam manajemen *cyberspace.* Internet dipandang sebagai sumber daya bersama yang memiliki kebebasan akses oleh siapa saja, sehingga aturan yang terdapat didalamnya juga merupakan hak bagi setiap orang. Tetapi, hal tersebut merupakan celah ancaman terhadap keamanan China.[211] Melalui *cyber sovereignty*, China memberikan legitimasi kepada negara kedaulatan untuk mengatur *cyberspace.* Pemerintah China memberikan keamanan *cyberspace* melalui kontrol yang dilakukan oleh negara. Sehingga, China seringkali memiliki permasalahan hak asasi manusia terkait kebebasan berpendapat. Membiarkan adanya *multi-stakeholder* dalam aturan tata kelola internet global hanya memunculkan para *stakeholder* yang dapat melawan otoritas yang dimiliki oleh pemerintah China.

5.3 *Cyber Issues* dalam Agenda Diplomatik Dialog Bilateral *Cybersecurity* China-AS

Pada saat China melakukan *cyberdiplomacy* dengan AS, terdapat beberapa agenda *cyber* yang diangkat sebagai isu yang tidak hanya mengenai persoalan keamanan teknis tetapi juga menggambarkan unsur politik. Meskipun terdapat perbedaan jalur diplomatik, yaitu track 1 dan track 1.5, pada umumnya agenda yang diangkat mengacu pada benang merah yang sama.

[211] Xinbao, Loc.cit.

5.3.1 *Cyber Agenda* dalam *US-China Cybersecurity Dialogue*

Tabel 5.1 ***Cyber Agenda US-China Cybersecurity Dialogue 2009-2015***

CICIR-CSIS Talks on Cybersecurity December 17, 2009		*US-China Cybersecurity Dialogue* an event co-hosted by CICIR and CSIS May 12 , 2010	*US-China Cybersecurity Dialogue* May 30, 2011	CICIR - CSIS Talks on Cybersecurity November 30 – December 1, 2011
Cyberspace and International Security	• National perspectives on cybersecurity • Principles, norms and lexicon for international security for cyberspace • Multilateral approaches to future Estonia-like incidents	• State behavior in cyberspace • National sovereignty application • International governance structure • Roles of technology and trade in cybersecurity • Appropriate rules for military conflict in cyberspace • Basis for cooperation on combating cyber crime	• Use of force in cyberspace • Law enforcement cooperation • Supply chain and trade issues • Governance in cyberspace • Sino-US trust in cyberspace	• Chinese and US Perspectives on developments in cybersecurity • National Practices and policies for cybersecurity • Military and Security issues in bilateral cybersecurity • Framework for international security in syberspace • Building strategic trust in cyberspace
Multilateral and National Activities to Promote Cybersecurity	• Securing the global cyber infrastructure • Cooperative approaches to cybercrime • Confidence-building in cyberspace			

US-China Cybersecurity Dialogue June 13-14 2012	CICIR - CSIS Talks on Cybersecurity December 4-5, 2012	*US-China Cybersecurity Dialogue* Cosponsored by CICIR and CSIS June 19-20, 2013	CSIS-CICIR Cybersecurity Dialogue February 2-3, 2015
• China-U.S. Confidence Building in the Cyberspace • International Norms and Cooperation over the Cyberspace • Law Enforcement Cooperation • New Risks, New Threats then New Concepts	• US perceptions of China's cyber security policy, Chinese perceptions of US cyber security policy • US and Chinese perceptions of international cyber environment • The Future of interdependence between the U.S and China: Implications of cybersecurity. • Boundaries of acceptable behavior in cyberspace. • Defining stability in cyberspace and measures to increase it • Improving crisis management for cyber security.	• Chinese and US Expectations for Responsible State Behavior • Mechanisms for Avoiding Miscalculation • Cooperative Measures to Increase Stability • Chinese and American Views on the Link between Security and Governance • Dealing with common threats • Track Two Cybersecurity Dialogue after the establishment of official working group	• The Use of Force in cyberspace • Fundamental principles for sovereignty, stability, and state responsibility • Norms for Cyberspace • Communication and Cooperation in Cyber incidents: Sony as a Case Study

Sumber : Disusun penulis berdasarkan laporan yang diterbitkan oleh *Center for Strategic and International Studies* (CSIS).[212]

[212] Agenda yang tidak dicantumkan oleh CSIS bersifat rahasia. Sumber pengolahan informasi disadur dari Center for Strategic and International Studies (CSIS), *Track 1.5 U.S.-China Cyber Security Dialogue*, 2009-2015, < https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/other-projects-cybersecurity/track-1> [accessed 19 September 2018].

Pada pertemuan pertama *U.S.-China Cybersecurity Dialogue,* agenda yang menjadi pokok pembahasan terbagi menjadi dua sesi. Sesi pertama membahas perihal *cyberspace* dan keamanan internasional. Sebagai awalan, keduanya saling memberikan pandangan terkait prinsip dan norma *cyberspace* yang berkaitan dengan persoalan keamanan internasional. Setiap negara memiliki perspektif, prinsip dasar maupun nilai dan norma yang berbeda terkait *cyberspace*, begtiu juga dengan China dan AS. Persoalan *cybersecurity* dilanjutkan dengan membahas insiden serangan *cyber* Estonia dan upaya multilateral yang dapat dilakukan sebagai antisipasi kedepannya. Dalam sesi kedua, pembahasan berada pada seputar upaya multilateral dan aktivitas nasional untuk meningkatkan *cybersecurity.* Agenda pada saat itu ialah pengamanan terhadap infrastruktur siber global, kerjasama untuk menghadapi kasus *cybercrime,* dan *confidence building.*

Agenda pertemuan kedua mulai memasuki pembahasan perilaku dan tata kelola *cyberspace.* Perilaku negara menjadi agenda pembuka dalam pertemuan tersebut. Keduanya mulai merumuskan perilaku negara mengenai apa yang boleh dan tidak boleh dilakukan oleh negara. Dalam pertemuan ini, salah satu perilaku yang disebutkan adalah penggunaan militer dalam *cyberspace.* Agenda mengenai konflik militer *cyberspace* dibahas dalam diskusi mengenai bentuk penerapan hukum internasional sebagai resolusi konflik. Pembahasan selanjutnya adalah mengenai struktur tata kelola internet internasional. Keduanya saling mengungkapkan pandangan terkait seperti apa struktur tata kelola internet yang baik bagi masyarakat internasional.

Masih dengan dialog yang sama, peran teknologi dan perdagangan dalam *cybersecurity* menjadi agenda kelima. Pembahasan berada pada topic seputar pengaruh teknologi dan perdagangan terhadap hubungan *cybersecurity* kedua negara, contohnya adalah hegemoni dalam bidang teknologi dan tekno-nasionalisme. Agenda dilanjutkan dengan pembahasan terkait kedaulatan nasional dalam *cyberspace*, dan juga kerjasama dalam menghadapi *cybercrime.*

Agenda pada pertemuan ketiga tidak memiliki laporan resmi yang dikeluarkan oleh CSIS. Tetapi, dalam artikelnya, CSIS menjelaskan bahwa beberapa agenda yang menjadi pembahasan sebelum pertemuan keempat adalah langkah kooperatif *cybersecurity*, tata kelola *cyberspace*, hubungan antara kedaulatan dan tanggung jawab nasional, pembentukan norma dan penggunaan kekuatan dalam *cyberspace*.[213] Agenda tersebut kemudian dikembangkan melalui pertemuan selanjutnya.

Pertemuan keempat diawali dengan agenda penggunaan kekuatan dalam *cyberspace.* Isi pembahasannya meliputi prinsip dasar, konsep, kriteria dan proses dari penggunaan kekuatan itu sendiri. Selanjutnya, dibahas mengenai kerjasama di bidang penegakan hukum dan permasalahan rantai suplai dan isu perdagangan. Mengenai masalah rantai suplai, CICIR dan CSIS mengemukakan bahwa keduanya saling mengkhawatirkan adanya eksploitasi terhadap rantai suplai masing-masing. Karena, hal tersebut dapat menyebabkan kelemahan jaringan dan infrastruktur

[213] James Andrew Lewis, '4th Meeting of the CSIS-CICIR Cybersecurity Dialogue', *the Center for Strategic and International Studies (CSIS),* 2011, <https://www.csis.org/events/4th-meeting-csis-cicir-cybersecurity-dialogue> [accessed 19 September 2018].

milik China maupun AS diketahui oleh satu sama lain.[214] Agenda mengenai rantai suplai ini masih membutuhkan diskusi dalam dialog lainnya.

Pembahasan dalam pertemuan keempat berlanjut dalam agenda-agenda lainnya. Agenda ketiga berada pada pembahasan mengenai pemerintahan *cyberspace*, yaitu hal-hal yang berkaitan dengan kesepakatan bilateral, institusi yang mengatur, kedaulatan dan tanggung jawab negara, serta norma dalam *cyberspace.* Terakhir adalah agenda tingkat kepercayaan China dan AS terhadap satu sama lain dalam *cyberspace.* Partisipan menjelaskan krisis kepercayaan yang dialami masing-masing pihak dan pengaruh tantangan yang ada dalam *cyberspace* terhadap tingkat kepercayaan itu sendiri. Kemudian, didiskusikan mengenai langkah-langkah apa saja yang dapat diambil sebagai jalur kerjasama dalam *cybersecurity*, dan upaya *Confidence Building Measure* atau CBM.

Transparansi terkait kebijakan nasional di bidang *cybersecurity* kembali menjadi agenda pada pertemuan kelima. Sebelumnya, partisipan hanya memberikan pandangan terhadap norma dan prinsip, lalu dilanjutkan dengan pandangan terkait kedaulatan. Kali ini, keduanya saling memberi informasi terkait kebijakan nasional dan strategi *cybersecurity.* Perwakilan AS, yaitu CSIS terlebih dahulu memperkenalkan *U.S. International Strategy for Cybersecurity.* Strategi tersebut menjelaskan bahwa *cyberspace* adalah salah satu ranah bagi AS untuk mencapai kepentingan nasionalnya. Sedangkan perwakilan dari pihak China menjelaskan kebijakan internet China berdasarkan *White Paper on China's Internet Policy*, dan proposal China pada saat diplomasi multilateralnya dalam bentuk

[214] CICIR & CSIS, Loc.cit.

China-Russia cosponsored International Code of Conduct for Information Security.[215] Dokumen terakhir kembali mengandung penegasan tentang hak kedaulatan negara untuk bertanggung jawab terhadap kebijakan internetnya masing-masing.

Agenda lainnya dalam pertemuan kelima *U.S.-China Cyber Security Dialogue* adalah pandangan terhadap perkembangan *cybersecurity.* Agenda tersebut diikuti dengan pembahasan terkait isu keamanan dan penggunaan militer dalam *cybersecurity* menjadi agenda selanjutnya. Isu keamanan tidak hanya membahas permasalahan didalamnya, tetapi juga kerangka keamanan internasional dalam *cyberspace,* dan bagaimana keduanya mengembangkan kepercayaan dalam *cyberspace* untuk menangani permasalahan keamanan itu sendiri. Permasalahan keamanan internasional yang menjadi isu keamanan bersama yaitu potensi serangan yang dapat dilakukan melalui *cyberspace.*

Pembahasan dalam sesi pertama pertemuan keenam adalah agenda *confidence building* yang dapat dilakukan China dan AS dalam *cyberspace.* Pada saat itu, CICIR dan CSIS membahas hal-hal apa saja yang dapat menghalangi China dan AS untuk meningkatkan kepercayaan terhadap satu sama lain. Lalu, keduanya mendiskusikan langkah-langkah yang dapat diambil sebagai upaya *confidence building.* Kedua belah pihak meyakini bahwa telah ada kemauan keduanya untuk meningkatkan kepercayaan dan kerjasama. Beberapa area yang mendapatkan dukungan dari perwakilan China untuk mencapai kerjasama adalah perlindungan

[215] CICIR & CSIS, Loc.cit.

terhadap infrastruktur kritis dan perlawanan terhadap aktivitas *cybercrime.*[216] Agenda CBM pada pertemuan kali ini merupakan pengembangan dari agenda CBM dan masalah isu kepercayaan yang dialami China dan AS pada pertemuan pertama dan keempat sebelumnya.

Norma internasional dan kerjasama dalam *cyberspace* menjadi agenda tersendiri dalam sesi kedua. Keduanya mendiskusikan perihal kode etik sebagai norma yang mengatur perilaku negara, dimana norma yang ada seharusnya dapat disepakati secara internasional. Tidak hanya itu, dibahas pula wadah yang dapat digunakan untuk membangun norma dan kode etik tersebut, seperti halnya GGE dan wadah internasional lainnya. Agenda mengenai norma internasional kemudian dilanjutkan oleh agenda kerjasama dalam bidang penegakan hukum pada sesi ketiga.

Perumusan resiko, ancaman, dan konsep-konsep baru dalam *cyberspace* menjadi agenda terakhir pada pertemuan keenam. Pembahasan didalamnya yaitu perihal relevansi teori yang ada untuk menjelaskan fenomena yang terjadi dalam *cyberspace.* Hal tersebut dikarenakan oleh sifat *cyberspace* sebagai ranah yang selalu berkembang dengan pesat. Lalu, penting bagi keduanya untuk dapat memiliki pemahaman bersama mengenai *cybersecurity*, dan segala standar yang dibutuhkan untuk menjelaskan sebuah fenomena.

Agenda selanjutnya adalah pembahasan mengenai resiko dan ancaman *cyberspace* yang dapat berasal dari perilaku negara dan aktor non-negara. Satu hal

[216] Adam Segal, *U.S. and China in Cyberspace: Uneasy Next Steps*, 2012, <https://www.cfr.org/blog/us-and-china-cyberspace-uneasy-next-steps> [accessed 19 September 2018].

yang disadari keduanya adalah bahaya yang ditimbulkan oleh aktor non-negara seperti kelompok terorisme.[217] Kejahatan finansial, penipuan dan kasus pornografi anak juga menjadi kasus kriminal lain yang harus dilawan. Untuk menghadapi ancaman keamanan *cyberspace,* pemerintah memiliki andil yang sangat penting. Keputusan pemerintah nantinya dapat berpengaruh terhadap legitimasi pengembangan kapabilitas *cyberspace* sebagai alat perang. Sebagai penutup, partisipan melakukan simulasi scenario ancaman *cyberspace* dan langkah yang diambil keduanya untuk menghadapi ancaman tersebut.

Pertemuan ketujuh diawali dengan agenda mengenai persepsi terhadap kebijakan *cybersecurity*. CICIR dan CSIS masing-masing memberikan penjelasan mengenai persepsi kebijakan *cybersecurity* milik negaranya satu sama lain dan saling memberikan tanggapan. Pembahasan kemudian dilanjutkan dengan agenda mengenai persepsi terhadap lingkungan *cyber* internasional, seperti halnya perkembangan agenda *cyber* dalam forum regional *Organization for Security and Cooperation in Europe* (OSCE).

Sesi kedua dilanjutkan dengan agenda mengenai masa depan hubungan interdependensi antara China dan AS. Topik diskusi pada saat itu ialah kerjasama China dan AS dalam bidang perdagangan dan teknologi. Permasalahan keduanya terletak pada masalah rantai suplai, data dan komputasi awan, dan tata kelola internet. Dalam hal ini, CICIR sebagai perwakilan negara China mengatakan bahwa China masih bergantung dalam hal pengembangan teknologi dengan AS.[218] Lebih

[217] CICIR & CSIS, Loc.cit.
[218] Harold, Libicki, & Cevallos, Loc. Cit.

lanjut, mereka mengatakan bahwa AS masih lebih unggul dari China, terutama dalam hal kemajuan teknologi informasi, sehingga beberapa sistem informasi China masih bergantung pada perusahaan AS. Untuk itu, kekhawatiran AS terhadap serangan *cyber* maupun rantai suplainya dalam wilayah China dianggap tidak berdasar.[219]

Agenda selanjutnya dalam pertemuan ketujuh ini adalah batasan perilaku negara dalam *cyberspace*. Agenda tersebut mendiskusikan perihal norma dan ekspektasi kedua belah pihak mengenai segala aspek dalam *cyberspace.* Didalamnya juga dibahas mengenai kerjasama dalam bidang penegakan hukum, sebagai kelanjutan dari pembahasan sebelumnya. Setelah batasan perilaku negara, agenda yang menjadi topic pembahasan adalah stabilitas dalam *cyberspace.* Keduanya merumuskan definisi stabilitas dalam *cyberspace,* dan tindakan-tindakan yang dapat diambil untuk mewujudkannya. Agenda yang menutup pertemuan ketujuh ini ialah agenda manajemen krisis *cybersecurity*, yang dilakukan pada satu hari setelahnya. Diskusi yang diangkat yaitu mengenai unsur-unsur dalam manajemen krisis dan peningkatan komunikasi bilateral. Keduanya kemudian melakukan simulasi scenario serangan siber untuk kedua kalinya.

Pada pertemuan kedelapan, dialog diawali dengan kedua belah pihak saling memberikan penjelasan singkat mengenai perkembangan kebijakan *cybersecurity* yang dimiliki oleh negara masing-masing. Keduanya kemudian membahas agenda perilaku negara yang bertanggung jawab dalam *cyberspace.* Agenda pada sesi kedua membahas mekanisme yang dapat dilakukan untuk menghindari adanya

[219] Harold, Libicki, & Cevallos, Loc cit.

salah perhitungan mengenai serangan *cyber*. Agenda dilanjutkan dengan pembahasan mengenai langkah-langkah kooperatif yang dapat diambil untuk meningkatkan stabilitas pada sesi ketiga. Sedangkan pada sesi keempat, keduanya saling memberikan pandangan terkait bagaimana hubungan antara keamanan dengan pemerintahan. Pada hari selanjutnya, agenda yang dibahas mengenai upaya yang dapat diambil China dan AS dalam menghadapi ancaman *cyber.* Agenda ditutup dengan membahas kelanjutan dari dialog track 1.5 antara CICIR dan CSIS, mengingat telah dibentuknya *working group* yang secara resmi membahas permasalahan *cybersecurity* oleh pemerintah kedua negara.

Agenda pertemuan kesembilan berada pada pembahasan mengenai penggunaan kekuatan dalam *cyberspace.* Dalam agenda tersebut, pembahasan meliputi prinsip dasar, konsep, kriteria dan proses dari penggunaan kekuatan itu sendiri. Sampai saat ini, belum ada kesepakatan internasional yang mendefinisikan sebuah insiden *cyber* sebagai serangan bersenjata, maupun penggunaan kekerasan (kekuatan). Sehingga konsep penggunaan kekuatan dalam *cyberspace*, agresi, kekuatan pertahanan, dan serangan bersenjata masih butuh untuk di tinjau ulang secara internasional. Sempat disinggung mengenai penggunaan hukum *Laws of Armed Conflict* (LOAC) sebagai hukum internasional yang berlaku untuk menyelesaikan permasalahan dalam *cyberspace*. Permasalahan LOAC masih menjadi perdebatan.[220]

Agenda dilanjutkan dalam pembahasan prinsip dasar atas kedaulatan, stabilitas, dan hubungan kedaulatan dengan tanggung jawab negara di bidang

[220] CICIR & CSIS, Loc.cit.

cybersecurity. Kedua belah pihak kemudian memberikan pandangan masing-masing mengenai kedaulatan dalam cyberspace, tanggungjawab negara di bidang *cybersecurity*, keseimbangan antara kedaulatan dan hak-hak universal, dan bagaimana kedaulatan mempengaruhi stabilitas. Salah satu isu dalam norma *cyberspace* yang berulangkali dikemukakan oleh CICIR sebagai perawakilan negara China adalah kedaulatan.[221]

Norma *cyberspace* kembali menajadi agenda dalam pertemuan ini. Agenda yang diangkat yaitu prinsip dasar dan kriteria terkait norma *cyberspace*, penerapan norma tersebut terhadap aktor non-negara dan bagaimana norma tersebut dapat berlaku sebagai komitmen internasional. Pertemuan ditutup dengan agenda mengenai komunikasi dan kerjasama dalam menghadapi insiden *cyber*. Tujuannya adalah untuk mengetahui dan mengidentifikasi langkah-langkah yang dibutuhkan, yang dapat meningkatkan komunikasi dan manajemen resiko atas insiden tersebut.

CSIS dan CICIR kembali melangsungkan dialog *cybersecurity* pada tahun 2017. Tetapi, laporan mengenai agenda dialog terakhir yang dirilis oleh situs resmi CSIS hanya berakhir pada pertemuan kesembilan. Adam Segal, salah satu perwakilan dari AS dalam dialog tersebut menceritakan agenda yang menjadi bahan diskusi pada saat itu. Agenda didalamnya adalah diskusi perihal keamanan *cyberspace*. Agenda tersebut dijelaskan melalui peristiwa *cyberspace* yang terjadi akhir-akhir ini. Topik yang diangkat adalah kasus intrusi Rusia terhadap hasil pemilihan umum presiden AS. Apabila mengurut pada pertemuan sebelumnya,

[221] Harold, Libicki, & Cevallos, Loc cit.

pertemuan pada tahun 2017 ini merupakan pertemuan yang kesepuluh dalam rangkaian pertemuan *U.S.-China Cyber Security Dialogue*.

CICIR yang mewakili China menekankan pada tiga poin utama.[222] Pertama, mereka tidak mempercayai AS yang menunjuk Rusia sebagai pelakunya. Karena seperti yang telah dijelaskan sebelumnya, China tidak mempercayai atribusi yang dilakukan oleh AS. Kedua, China tidak melihat upaya AS untuk menyelesaikan permasalahan *cybersecurity* dengan Rusia. AS hanya memberlakukan sanksi dan mengirim beberapa diplomat Rusia kembali ke negaranya.[223] Kritik yang kemudian timbul dari pemberlakuan sanksi adalah AS melakukan aksi unilateral sebagai respon terhadap kasus tersebut. China menolak adanya aksi sepihak seperti yang dilakukan AS, dan mengatakan bahwa aksi tersebut dapat menjadi penghalang dalam kerjasama untuk membentuk norma *cyberspace.*[224] Ketiga, kembali adanya penekanan bahwa China merupakan korban *cybercrime.* Telah disebutkan bahwa prinsip dasar yang dianut oleh China adalah non-intervensi. Sehingga, tidaklah seharusnya khawatir terhadap kapabilitas *cyber* China. Selain itu, memang sudah seharusnya China memberlakukan kontrol terhadap *cyberspace* untuk mencegah hal yang tidak diinginkan seperti yang terjadi pada pesta demokrasi AS.[225]

Agenda hubungan bilateral kedua negara sedikit banyak menjadi topic pembahasan. Pembahasan dimulai dengan diskusi mengenai kebijakan domestik

---

[222] Adam Segal, *The Continued Importance of the U.S.-China Cyber Dialogue*, 2017, <https://www.cfr.org/blog/continued-importance-us-china-cyber-dialogue> [accessed 23 September 2018].
[223] Ibid.
[224] Ibid.
[225] Adam Segal, *The Continued Importance of the U.S.-China Cyber Dialogue*, loc.cit., & Michael Sulmeyer, Amy Chang, *Three Observations on China's Approach to State Action in Cyberspace*, 2017, <https://www.lawfareblog.com/three-observations-chinas-approach-state-action-cyberspace> [accessed 23 September 2018].

China, yaitu *cybersecurity law*. Hukum tersebut dianggap mengancam perusahaan AS yang berada di wilayah China. Tetapi, dalam forum tersebut perwakilan China menjelaskan bahwa *cybersecurity law* tidak bermaksud untuk membatasi ruang gerak perusahaan asing, dan hanya bertujuan untuk meningkatkan *cybersecurity* negara China. Lalu, China mengatakan niatannya untuk memperluas kerjasama dalam bidang *cybersecurity*. China juga mengatakan kekhawatirannya mengenai kelanjutan diskusi *cybersecurity* di bawah pemerintahan presiden Trump.[226]

Pertemuan selanjutnya dilaksanakan pada bulan November tahun 2017. Pertemuan ini merupakan pertemuan kesebelas dari serangkaian pertemuan dalam *cybersecurity dialogue*. Agenda didalamnya adalah pembahasan mengenai norma *cyberspace*. Hukum internasional masih diperjuangkan sebagai jalan resolusi konflik dalam *cyberspace*. Dibahas pula mengenai hak bela diri atau *right of self defense* dan tanggung jawab perilaku negara, termasuk juga tindakan balasan sebagai respon menghadapi serangan *cyber*.[227] Respon yang diberikan perwakilan China pada saat masih sama seperti pembahasan LOAC sebelumnya. Mereka tidak setuju untuk memberlakukan LOAC. Partisipan perwakilan China mengatakan bahwa *cyberspace* merupakan domain konflik baru, sehingga lebih baik untuk membentuk aturan baru yang masih belum tercakup dalam hukum internasional. Meskipun telah gagal mencapai consensus dalam pertemuan terakhirnya, CICIR mendukung GGE sebagai forum utama dalam pembentukan norma *cyberspace*.

[226] Adam Segal, *The Continued Importance of the U.S.-China Cyber Dialogue*, loc.cit.
[227] Adam Segal, *An Update on U.S.-China Cybersecurity Relations*, 2017, <https://www.cfr.org/blog/update-us-china-cybersecurity-relations> [accessed 23 September 2018].

Agenda selanjutnya kembali mengangkat operasionalisasi *cyberspace* di bidang militer. Diksusi terkait agenda tersebut tidak mengalami banyak perubahan dari hasil sebelumnya. Belum ada kesepakatan mengenai batasan militer, mekanisme untuk memberikan sinyal, dan metode yang dapat dijadikan pengukur kontrol terhadap eskalasi konflik. Agenda lainnya adalah pembahasan mengenai LECD sebagai salah satu dialog empat pilar. Pada saat itu, perwakilan AS mengajukan agar lebih banyak PLA yang dapat terlibat dalam diskusi *cybersecurity,* dan menyarankan adanya forum dialog lainnya selain LECD. Sedangkan perwakilan dari pihak China mengajukan untuk tetap menggunakan dialog LECD.[228]

5.3.1.2 Joint Statement *U.S.-China Cyber Security Dialogue* tahun 2012

Pada bulan Juni tahun 2012, CICIR dan CSIS merilis *Joint Statement* dari *U.S.-China Cyber Security Dialogue*.[229] Melalui *joint statement,* terdapat gambaran sementara dialog bilateral yang dilakukan oleh kedua belah pihak, meskipun tidak dalam bentuk kesimpulan akhir. Dokumen tersebut dirilis setelah diadakannya pertemuan keenam.dialog *cybersecurity*. Sehingga *joint statement* ini hanya menggambarkan hasil dari agenda yang dibahas dalam enam kali pertemuan.

Pada saat *joint statement* tersebut dipublikasikan kepada publik, terdapat beberapa area yang belum dan sudah mencapai kesepakatan. Terlihat bahwa kedua belah pihak memiliki pandangan yang sama terkait tujuan diadakannya *U.S.-China Cyber Security Dialogue,* yaitu agar keduanya dapat menghindari adanya

[228] Ibid.
[229] CICIR & CSIS, Loc.cit.

kesalahpahaman antara satu sama lain terutama dalam hal *cybersecurity*. Kepercayaan dapat menjadi dasar hal yang dapat membawa keduanya terhindar dari konflik berkelanjutan. Sehingga keduanya juga menyepakati bahwa CBM dalam *cyberspace* merupakan hal yang sangat dibutuhkan untuk meningkatkan kepercaayaan tersebut. Keduanya berupaya mencari jalan untuk melakukan CBM. Pendapat yang muncul dalam beberapa upaya yang dapat dilakukan China dan AS dalam melakukan CBM adalah transparansi terhadap doktrin militer *cyberspace*, pertukaran kunjungan yang dilakukan oleh rakyat sipil maupun angkatan militer, pertukaran informasi mengenai ancaman *cyberspace,* deskripsi terhadap proses pengambilan keputusan, dan pelatihan bersama antara China dan AS.

Kedua belah pihak menyadari terdapat ancaman *cyberspace* yang lebih baik apabila dihadapi bersama. Ancaman terutama berasal dari aktor non negara, dengan bentuk yang paling berbahayanya yaitu kelompok terorisme. Keduanya kemudian menyepakati bahwa dibutuhkan adanya kerjasama dalam menghadapi *cybercrime.* Selain aksi terrorisme, disebutkan bahwa kasus *cybercrime* dalam bentuk kejahatan finansial, penipuan dan kasus pornografi anak merupakan kasus utama.

Dialog tersebut kemudian menghasilkan sinyal baik untuk melanjutkan pembahasan mengenai kerjasama. Hal itu diperlihatkan melalui kemajuan agenda kerjasama dalam bidang penegakan hukum. Tetapi, implementasi dari bentuk kerjasama tersebut dikatakan cukup sulit. Sebagai langkah pencegahan *cybercrime* lainnya, keduanya sepakat untuk melakukan pencegahan bersama dimulai dengan membangun jalur komunikasi untuk merespon insiden *cybercrime*.

CICIR dan CSIS sepakat untuk membentuk ranah *cybersecurity* yang berdasar pada hukum internasional untuk membentuk norma terkait perilaku cyberspace. Keduanya sepakat bahwa dibutuhkan adanya aturan *cybersecurity* yang berlaku secara internasional. Hal tersebut dapat diwujudkan melalui kesepakatan dalam bidang hukum internasional dan pembentukan norma bersama terkait perilaku negara dalam *cyberspace.* Yang masih menjadi perdebatan adalah norma seperti apa yang dapat diterima secara internasional. Bahkan kedua belah pihak masih mempertahankan prinsipnya sendiri terkait perilaku negara maupun keamanan dalam *cybersepace.*

Dijelaskan dalam *joint statement,* China, yang diwakilkan oleh CICIR mengajukan empat unsur kode etik dalam *cyberspace.*[230] Pertama adalah larangan penggunaan *cyberspace* sebagai senjata, termasuk juga menahan diri untuk tidak mengembangkan senjata *cyber*. Kedua, menghormati hak setiap negara untuk mengelola jaringan yang berada dalam wilayahnya sendiri, dan menolak hegemoni *cyberspace*. Ketiga, meningkatkan kepercayaan terhadap satu sama lain dengan berjanji untuk tidak menggunakan maupun mengembangkan senjata *cyber*. Keempat adalah membentuk badan pengelola internasional yang dapat mengatur distribusi sumber daya internet dengan adil. Badan yang dimaksud dapat didampingi oleh PBB seperti halnya IAEA, untuk meninjau dan menginvestigasi kasus serangan *cyber*. Kode etik yang diajukan China pada saat itu masih dalam tahap pertimbangan antara kedua belah pihak.

[230] CICIR & CSIS, Loc.cit.

Sedangkan CSIS menekankan pada agenda terkait pembentukan norma dan *confidence building* untuk meningkatkan stabilitas. Pihak CSIS sebagai perwakilan AS menyarankan adanya peningkatan terhadap transparansi, seperti halnya mempertemukan kepala negara China dan AS, perumusan upaya bersama untuk meningkatkan stabilitas, pengakuan terhadap LOAC sebagai jalur resolusi konflik, komitmen terhadap perlindungan hak kekayaan intelektual, dan penggunaan Konvensi Budapest untuk menghadapi *cybercrime.*

Beberapa agenda yang belum mencapai kesepakatan berada pada seputar norma terkait *cyberspace* dan resolusi terhadap tanggung jawab perilaku negara. China yang diwakili oleh CICIR membawa gagasan mengenai '*no-first-use agreement',* yaitu kesepakatan untuk tidak menggunakan senjata *cyber* antar negara. Selain itu, China juga menekankan pada kerentanan *cyberspace* yang dihadapi bersama pada saat ini merupakan alasan penting bagi setiap negara untuk saling bekerjasama. Sedangkan AS mendukung penggunaan hukum LOAC sebagai hukum internasional yang berlaku untuk menyelesaikan permasalahan dalam *cyberspace*. China tidak menyetujui LOAC yang digunakan AS sebagai legitimasi kepada negara untuk merespon serangan *cyber* sebagai konflik militer. Karena pada dasarnya, China tidak mempercayai atribusi serangan *cyber* yang dilakukan oleh AS, dimana China sendiri masih lemah dalam hal tersebut.[231]

CICIR mengungkapkan bahwa pada dasarnya, mereka menyadari pentingnya Konvensi Budapest terhadap *cybercrime.* Akan tetapi, China tidak menyetujui penggunaan Konvensi Budapest sebagai dasar hukum yang diakui

[231] Harold, Libicki, & Cevallos, Loc cit.

secara internasional. Konvensi tersebut dianggap belum mengakomodasi kerentanan yang dimiliki negara berkembang, bahwa intrusi dapat diarahkan pada negara yang memiliki sistem keamanan rendah. Investigasi yang akan dilakukan juga dapat melanggar kedaulatan terhadap kebijakan domestik suatu negara. China kemudian menyarankan bahwa forum internasional seperti GGE adalah jalur yang lebih tepat untuk membangun tata kelola dan norma *cyberspace.* China menganjurkan untuk membangun konvensi internasional baru terkait *cybercrime* yang dibentuk melalui upaya bilateral dan multilateral, diakui oleh GGE, dan berada di bawah kerangka PBB.

Mengenai norma *cyberspace*, terdapat perdebatan terkait prinsip kedaulatan. Salah satu isu dalam norma *cyberspace* yang berulangkali dikemukakan oleh China adalah kedaulatan.[232] China menyadari bahwa internet bersifat transnasional dan global, tetapi tetap saja mengandung unsur kedaulatan negara. Meskipun *cyberspace* adalah dunia maya, jaringan yang menghubungkan internet memiliki wujud dan saling terhubung dalam wilayah teritori di dunia nyata. Untuk itu, China berpendapat bahwa aturan yang mengatur kedaulatan wilayah juga berlaku dalam *cyberspace*, dan perlu bagi setiap negara untuk menerima kedaulatan sebagai prinsip dasar *cybersecurity.*[233] Dalam hal ini, AS tetap berteguh pada komitmennya secara internasional, yaitu memperjuangkan hak kebebasan berpendapat sesuai dengan konstitusi negaranya.

[232] Harold, Libicki, & Cevallos, Loc cit.
[233] CICIR & CSIS, Loc.cit.

Terakhir, CICIR dan CSIS sepakat untuk melanjutkan *cybersecurity dialogue* sebagai wadah diskusi terkait permasalahan *cybersecurity.* Keduanya mendukung terbentuknya kerjasama *cybersecurity* yang dapat dilakukan China dan AS, yang diawali dengan membentuk jalur komunikasi bilateral, dan kerjasama melalui CERT kedua negara. Lalu, keduanya sepakat untuk meningkatkan kesadaran masyarakat terhadap isu *cybersecurity*, dan mempublikasikan isu-isu dalam agenda yang telah didiskusikan oleh dialog ini.

5.3.2 *Cyber Agenda* dalam *U.S.-China Strategic and Economic Dialogue* (S&ED)

China dan AS pada akhirnya membentuk sebuah forum diplomatik bilateral track 1 untuk membahas isu *cybersecurity*. Sebelumnya, dialog bilateral China dan AS hanya dilakukan oleh segelintir perwakilan pemerintah. Akan tetapi, dalam dialog kali ini peran tersebut dilakukan oleh perwakilan kenegaraan. Keduanya bahkan berupaya untuk melanjutkan dialog bilateral dalam bentuk mekanisme CWG untuk mendiskusikan kerjasama *cybersecurity* lebih lanjut.

Salah satu agenda dalam S&ED kelima adalah memperkenalkan CWG sebagai wadah dialog bilateral dalam isu *cybersecurity.* Pada saat pertemuan CWG, pembahasan berada pada agenda untuk membangun kerjasama tim koordinasi permasalahan *cyberspace*, hubungan kedua belah pihak dalam permasalahan jaringan dan infrastruktur, aturan internasional dalam *cyberspace,* dan kelanjutan dialog bilateral mengenai langkah kerjasama *cybersecurity*.[234] Melalui CWG,

[234] Embassy of the People's Republic of China in the Republic of Kenya, Loc.cit.

diharapkan kedua belah pihak dapat meningkatkan kesepakatan terkait prinsip dan norma *cyberspace.* Agenda yang menjadi sorotan utama adalah isu *cybersecurity* dan perlindungan hak kekayaan intelektual. Pada saat itu, China menyatakan upayanya untuk meningkatkan perlindungan terhadap hak kekayaan intelektual dan rahasia dagang. Disebutkan bahwa China berkomitmen untuk menggunakan pernagkat lunak hasil badan usaha negaranya sendiri.[235]

Agenda lainnya adalah pembahasan mengenai upaya peningkatan kerjasama tim koordinasi bidang *cyber* atau yang disebut dengan *Computer Emergency Response Team* (CERT). Agenda mengenai koordinasi antar kelompok CERT telah ada sejak *US-China Cybersecurity Dialogue.*[236] Tetapi pada saat itu masih hanya berupa ide yang digagas sebagai upaya kerjasama yang dapat dilakukan kedua negara. Dibentuknya CWG menjadi awal dari pembentukan tim koordinasi CERT yang ada di kedua negara. Upaya pengembangan *cybersecurity* secara teknis terlihat pada persetujuan keduanya untuk melakukan konsultasi bersama yang akan dilakukan oleh *Computer Network Emergency Response Technical Team/Coordination Center of China* (CNCERT/CC) dan *the United States Computer Emergency Readiness Team (US-CERT).*[237]

Salah satu inisiasi yang muncul dalam melakukan kerjasama *cybersecurity* adalah pembentukan *cyber hotline.* China dan AS menyetujui untuk membentuk *hotline* dengan tujuan sebagai jalur komunikasi antar kepala negara dalam

[235] U.S. Department of the Treasury, *U.S. Fact Sheet – Economic Track Fifth Meeting of the U.S.-China Strategic and Economic Dialogue*, 2013, < https://www.treasury.gov/press-center/press-releases/Pages/jl2011.aspx> [accessed 24 September 2018].
[236] CICIR & CSIS, Loc.cit.
[237] Embassy of the People's Republic of China in the United States of America, *U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track,* Loc.cit.

merespon permasalahan *cybersecurity*.[238] Berbeda dengan *US-China cybersecurity dialogue,* agenda *cyber hotline* yang dibawa dala forum ini menjadikan keberadaan *cyber hotline* sebagai bentuk perkembangan dalam kerjasama *cybersecurity* China dan AS. Dialog kelima S&ED kembali menyebutkan upaya penegakan hukum bersama dalam beberapa area prioritas isu *cybercrime,* antara lain adalah pencurian hak kekayaan intelektual, penipuan *cyber* dan juga kasus pornografi anak.[239] Selain itu, agenda dalam CWG mulai memasukkan perlawanan terhadap terorisme, meskipun masih belum secara spesifik. Keduanya sepakat untuk melakukan pembahasan lebih lanjut terkait isu *cybersecurity.*

5.3.3 *Cyber Agenda* dalam Kunjungan Kenegaraan Presiden Xi Jinping ke Amerika Serikat

Pada saat presiden Xi Jinping melakukan kunjungan ke Washington, beliau bersama dengan presiden Obama berbicara mengenai berbagai agenda dalam hubungan bilateral kedua negara. Topik pembicaraan keduanya meliputi model hubungan baru antara China dan AS, kerjasama bilateral, permasalahan asia-pasifik, dan tantangan global dalam hubungan keduanya. Pembicaraan tersebut kemudian membuahkan kesepakatan dalam beberapa isu, diantaranya adalah isu *cybersecurity.* Agenda yang menjadi fokus pembahasan dalam bagian ini berfokus pada agenda yang berkaitan dengan isu *cybersecurity* pada saat kunjungan tersebut

[238] Embassy of the People's Republic of China in the United States of America, *U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track,* Loc.cit.
[239] Embassy of the People's Republic of China in the United States of America, *U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track,* Loc.cit.

dilakukan, yaitu kesepakatan *cybersecurity* yang tercapai antara China dan AS pada tahun 2015.

Kesepakatan tersebut menekankan bahwa keduanya sepakat untuk tidak melakukan maupun mendukung aktivitas pencurian hak kekayaan intelektual atau yang disebut dengan EMCE. Seperti yang telah dijelaskan sebelumnya, keduanya saling tuduh-menuduh terkait aktivitas EMCE. China menolak untuk mengakui aturan mengenai EMCE yang dibuat oleh AS.[240] China berpendapat bahwa AS tidak memiliki hak dalam membentuk norma EMCE dalam *cyberspace,* dimana ia sendiri juga merupakan pelaku dari spionase siber.[241] Terlebih lagi, didalam hukum internasional tidak ada aturan yang membedakan aktivitas spionase siber tradisional dengan EMCE. Tetapi dengan menyetujui kerjasama tersebut maka posisi China terhadap EMCE pun turut mengalami perubahan.

Beberapa *cyber agenda* yang dapat disimpulkan dalam kerjasama tersebut adalah agenda mengenai kerjasama bilateral *cybersecurity,* pembentukan norma *cyberspace*, dan isu *cybercrime.* Pertama adalah kerjasama bilateral *cybersecurity.* Selain kesepakatan dalam hal EMCE, keduanya lalu mengembangkan suatu kerjasama bilateral. Kedua belah pihak sepakat untuk bekerjasama dalam bidang investigasi dan pertukaran informasi terkait *cybercrime.* Kerjasama tersebut masih berupaya menentukan mekanisme dan prosedur permintaan bantuan investigasi. Agenda kerjasama lainnya membahas kerjasama dalam pembentukan mekanisme *cyber hotline* sebagai bagian dari mekanisme kerjasama pertukaran informasi.

[240] Harold, Libicki, & Cevallos, Loc cit
[241] Hurwitz, Op.cit.

Agenda selanjutnya adalah pembahasan mengenai norma *cyberspace.* Kedua belah pihak berupaya mencapai kesepakatan terhadap norma *cyberspace* yang dapat diterima secara internasional. Dalam kesepakatan tersebut disebutkan bahwa China dan AS menerima laporan hasil pertemuan GGE pada tahun 2015.[242] Dokumen tersebut berisi penjelasan mengenai isu keamanan internasional dalam *cyberspace,* begitu juga dengan norma yang berlaku didalamnya. Lalu, keduanya sepakat untuk membentuk kelompok tenaga ahli yang akan berfokus pada isu terkait norma *cyberspace.*

Agenda mengenai isu *cybercrime* akan dilanjutkan dalam dialog tingkat tinggi sebagai kelanjutan dari kerjasama ini. Keduanya sepakat membentuk *high-level joint dialogue mechanism on fighting cybercrime and related issues*, yaitu sebuah forum bilateral yang berfokus pada permasalahan isu *cybersecurity* dan *cybercrime.* Disebutkan dalam hasil pertemuan presiden Xi dan presiden Obama, bahwa dalam forum tersebut China akan mengirimkan delegasi yang berasal dari kementrian dalam pemerintahannya untuk memimpin jalannya dialog, dan beberapa perwakilan dari kementrian lainnya sebagai partisipan. Sedangkan AS akan mengirimkan perwakilan dari Departemen Keamanan Dalam Negeri untuk memimpin dialog dan perwakilan FBI sebagai partisipannya.[243]

[242] The Ministry of Foreign Affairs of the People's Republic of China, *Full Text: Outcome list of President Xi Jinping's state visit to the United States,* Loc.cit.
[243] The Ministry of Foreign Affairs of the People's Republic of China, *Full Text: Outcome list of President Xi Jinping's state visit to the United States,* Loc.cit.

5.3.4 *Cyber Agenda* dalam *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*

Tabel 5.2 Summary of Outcomes U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues

First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues	Second U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues	Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues
Guidelines for Combatting Cybercrime and Related Issues Tabletop Exercise Hotline Mechanism Enhance Cooperation on Combatting Cyber-Enabled Crime and Related Issues Second U.S.-China High Level Joint Dialogue on Cybercrime and Related Issues	Tabletop Exercise Hotline Mechanism Network Protection Information Sharing, Case Cooperation, and Resources Cyber-Enabled Crime Senior Expert Group Third U.S.-China High Level Joint Dialogue on Cybercrime and Related Issues.	Combatting Cybercrime and Cyber-Enabled Crime Network Protection Misuse of Technology and Communications to Facilitate Violent Terrorist Activities Hotline Mechanism Dialogue Continuity

Sumber: Disusun penulis berdasarkan laporan yang diterbitkan oleh *U.S. Department of Justice*[244]

U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues merupakan bentuk kelanjutan dari kerjasama *cybersecurity* yang telah disepakati pada tahun 2015. China dan AS sebelumnya berkomitmen untuk bekerjasama dalam perlindungan jaringan, termasuk memelihara dan meningkatkan keamanan

[244] U.S. Department of Justice, *First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes*, 2015, <https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialoguecybercrime-and-related-issues-summary-outcomes-0>, U.S. Department of Justice, *Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue*, 2016, https://www.justice.gov/opa/pr/second-us-china-cybercrime-andrelated-issues-high-level-joint-dialogue, & U.S. Department of Justice, *Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*, 2016, <https://www.justice.gov/opa/pr/third-us-china-highlevel-joint-dialogue-cybercrime-and-related-issues> [accessed 24 September 2018],

informasi *cyberspace*, serta mengambil aksi nyata dalam menangani isu *cybercrime.* Dialog tingkat tinggi ini diadakan sebanyak tiga kali dalam kurun waktu satu tahun setelah tercapainya kerjasama *cybersecurity.* Pertemuan pertama diadakan hanya berjarak tiga bulan setelah kerjasama tersebut mencapai kesepakatan, yakni tepat pada bulan Desember tahun 2015. Pertemuan kedua diadakan pada bulan Juni tahun 2016. Pertemuan ketiga diadakan pada tahun yang sama, tepatnya pada bulan Desember tahun 2016. Tabel 5.2 menunjukkan perkembangan agenda dalam tiga pertemuan dialog ini.

5.3.4.1 Agenda dalam *First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*

Pada pertemuan pertama, berhasil dibentuk dokumen terkait pedoman permintaan asistensi terhadap kasus *cybercrime* dan prosedur pemenuhan permintaan bantuan. Keduanya sepakat untuk saling berbagi petunjuk dan informasi terkait kasus *cybercrime* yang terjadi di masing-masing negara, dengan prosedur dan waktu yang ditentukan. Fungsi dari dokumen tersebut adalah memberikan pemahaman bagi kedua belah pihak terkait informasi apa saja yang dapat diberikan. Selain itu, diatur pula mengenai tenggat waktu untuk merespon permintaan investigasi.

Agenda dilanjutkan dengan pembahasan mengenai latihan meja atau *tabletop exercise. Tabletop exercise* dilakukan melalui skenario langkah yang dapat diambil ketika menghadapi permasalahan yang diangkat, serta peranan penting yang ada di dalamnya. Tujuannya adalah untuk meningkatkan pemahaman kedua belah pihak mengenai proses dan prosedur dalam mengatasi kasus *cybercrime* dan isu terkait

lainnya. Rencananya, *tabletop exercise* pertama akan dilaksanakan pada tahun 2016, dengan berfokus pada permasalahan *cybercrime*, aktivitas *cyber* berbahaya, dan skenario perlindungan jaringan. Agenda ketiga membahas perkembangan inisiasi pembentukan *cyber hotline*. Dalam pertemuan ini, keduanya sepakat untuk melanjutkan diskusi mengenai cakupan, tujuan, dan prosedur dari penggunaan *hotline* tersebut dan mencapai kesepakatan sebelum pertemuan selanjutnya.

Agenda keempat adalah peningkatan kerjasama dalam melawan *cyber-enabled crime*[245] dan isu-isu terkait. Kedua belah pihak sepakat untuk mengembangkan kerjasama melalui kasus yang ada untuk menghadapi berbagai kejahatan dunia maya termasuk juga kasus eksploitasi anak, pencurian rahasia dagang, penipuan, dan penyalahgunaan teknologi dan jalur komunikasi untuk aktivitas terorisme. Sebagai langkah peningkatan keamanan, keduanya akan mengembangkan pertukaran tenaga ahli dalam hal perlindungan jaringan. Rencananya, tenaga ahli China dan AS dijadwalkan untuk bertemu pada 3 Desember 2015. Pertemuan tersebut akan dikembangkan menjadi pertemuan berkala dalam pembahasan dialog selanjutnya, yang telah disepakati untuk diadakan di Beijing pada bulan Juni tahun 2016.

5.3.4.2 Agenda dalam *Second U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*

Agenda yang membuka pertemuan kedua ini adalah pembahasan *tabletop exercise* yang telah diadakan pada bulan April tahun 2016 silam. Latihan tersebut

[245] ***Cyber-enabled crime*** adalah salah satu jenis *cybercrime* yang dibedakan sebagai kejahatan tradisional yang didukung oleh penggunaan *cyberspace*. Sehingga, tindakan kejahatan dapat dilakukan meskipun tidak menggunakan internet. Dikutip dari Interpol, *Cybercrime*, <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> [accessed 25 September 2018],

telah dijalankan dengan efektif, sehingga kedua belah pihak sepakat untuk melakukan *tabletop exercise* yang kedua. Fokus yang diambil masih sama, yakni seputar pelatihan untuk menghadapi *cybercrime* dan perlindungan jaringan. Kepastian dari agenda ini akan didiskusikan kembali dalam dialog selanjutnya.

Pertemuan ini kembali membahas mekanisme *hotline* sebagai agenda kedua. Kedua belah pihak telah mencapai ksepekatan mengenai cakupan, tujuan dan prosedur dari pembentukan *hotline* dalam pertemuan kedua dialog tingkat tinggi AS-China terkait permasalahan *cybercrime*. Sebelumnya, kesepakatan tersebut masih sebatas perencanaan saja. Mekanisme pembentukan jaringan *hotline* berada dibawah rencana kerja *U.S.-China Cybercrime and Related Issues Hotline Mechanism*.[246] Pertemuan ini juga menyepakati uji coba mekanisme *cyber hotline* yang akan dilakukan sebelum bulan September tahun 2016.

Agenda ketiga ialah agenda perlindungan jaringan. Langkah yang diambil oleh keduanya diawali dengan menyelenggarakan seminar mengenai keamanan dan perlindungan jaringan yang diadakan pada bulan Agustus 2016. Seminar tersebut ditujukan bagi para ahli yang bergerak di bidang *cybersecurity*. Kedepannya, pertemuan tersebut akan dijadikan pertemuan secara berkala.

Agenda selanjutnya yaitu perihal kerjasama di bidang bantuan investigasi dan pertukaran informasi. Kedua belah pihak menyepakati beberapa keputusan terkait langkah kerjasama yang akan dibangun. Pertama adalah mengembangkan kerjasama dalam bentuk jaringan informasi. Kerjasama tersebut dilakukan dalam

[246] U.S. Department of Justice, *Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue*, 2016, https://www.justice.gov/opa/pr/second-us-china-cybercrime-andrelated-issues-high-level-joint-dialogue> [accessed 24 September 2018].

bidang investigasi maupun pertukaran informasi terkait *cybercrime* dan aktivitas *cyber* berbahaya lainnya. Kedua, melakukan pertukaran informasi dan meningkatkan kerjasama dalam menangani kasus *cybercrime*. Ketiga, mengadakan diskusi mengenai pertukaran informasi dan hubungannya dengan Perjanjian Bantuan Hukum Timbal Balik atau *Mutual Legal Assistance Agreement* (MLAA). Keempat, meningkatkan pertukaran informasi yang berkaitan dengan ancaman *cyber*. Informasi akan diberikan dan dilaporkan secara berkala, termasuk juga informasi mengenai sampel *malware* dan sejenisnya. Di bawah MLAA kemudian akan dibangun mekanisme komunikasi dan pembentukan otoritas pusat. Mekanisme tersebut akan menggunakan *The 24/7 High Tech Network of international points of contact*[247], sebagai jalan untuk memberikan bantuan penyelidikan dalam bentuk bukti elektronik. Kegunaan dari titik poin kontak internasional salah satunya adalah bantuan untuk melibatkan bantuan dari aparat penegak hukum negara lainnya.

Agenda yang kelima adalah diskusi terkait kejahatan dunia maya. Upaya melawan *cybercrime* dilakukan melalui inisiasi kerjasama penegakan hukum dalam empat area. Pencurian rahasia dagang dan kekayaan intelektual masih menjadi area prioritas. Untuk kasus penipuan siber, China dan AS telah sampai pada pembentukan rencana aksi untuk mengantisipasi *business email compromise* (BEC). Beberapa agenda penanggulangan kasus prioritas lainnya yaitu kasus

[247] *The 24/7 High Tech Network of international points of contact*, yaitu jaringan dari titik-titik kontak internasional yang bekerja selama 24 jam setiap harinya. DIkutip berdasarkan Chris Ott, 'What You Should Know About The 24/7 Cybercrime Network', Davis Wright Tremaine LLP, 2018, <https://www.dwt.com/files/uploads/documents/publications/What%20You%20Should%20Know%20About%20The%2024.pdf> [accessed 27 September 2018].

distribusi pornografi anak, penyalahgunaan internet untuk tujuan terorisme dan perdagangan senjata api *online.* Informasi mengenai kasus penyalahgunaan internet untuk kegiatan terorisme dilakukan melalui seminar berkelanjutan mengenai penyalahgunaan teknologi dan komunikasi untuk aktivitas terorisme pada tahun 2016.

Terakhir adalah agenda pembentukan *senior expert group.* Selain tim koordinasi CERT, China dan AS berencana untuk membentuk kelompok tenaga ahli pertama yang akan berfokus pada norma internasional *cyberspace* dan isu-isu terkait lainnya. Perwakilan China dan AS pada saat itu sepakat untuk melanjutkan dialog ketiga yang berlokasi di Washington, D.C. Pelaksanaan pertemuan tersebut diagendakan pada pertengahan tahun 2016.

5.3.4.3 Agenda dalam *Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*

Upaya melawan *cybercrime* dan *cyber-enabled crime* menjadi agenda pertama dalam pertemuan ketiga *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*. Melanjutkan komitmen sebelumnya, perwakilan China dan AS yang hadir dalam dialog tersebut setuju untuk meningkatkan kerjasama dalam hal investigasi dan mencegah pencurian hak kekayaan intelektual. Terdapat empat bentuk upaya untuk meningkatkan kerjasama.[248] Pertama, disebutkan bahwa mekanisme *"Status Report on U.S./China Cybercrime Cases"* akan tetap dilanjutkan untuk mengevaluasi efektivitas dialog kerjasama. Lalu,

[248] U.S. Department of Justice, *Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*, 2016, <https://www.justice.gov/opa/pr/third-us-china-highlevel-joint-dialogue-cybercrime-and-related-issues> [accessed 24 September 2018],

Kerjasama dalam menghadapi kasus peretasan dan penipuan dunia maya, dan distribusi pornografi anak juga akan dilanjutkan. Bentuk kerjasama tersebut kemudian akan ditambah dengan perlawanan terhadap aktivitas perdagangan obat-obatan terlarang maupun senjata api yang dijual di pasar gelap secara *online*. Keduanya juga akan menentukan area prioritas untuk kelanjutan rencana kerjasama dalam bidang penegakan hukum. Ketiga, keduanya berupaya untuk menyediakan pembaruan terhadap kasus-kasus yang menjadi agenda dialog secara kongkrit dan tepat waktu. Keempat, diskusi mengenai wadah kerjasama multilateral akan tetap dilanjutkan.

Perlindungan jaringan kembali dibahas sebagai agenda pertemuan ketiga ini. Seminar yang mengangkat topik perlindungan jaringan telah berhasil dilaksanakan. Pembahasan mengenai perlindungan jaringan lalu disarankan agar dapat dilakukan secara berkelanjutan. Kemudian pembahasan dilanjutkan pada upaya-upaya perlindungan jaringan yang dapat dilakukan oleh China maupun AS. Upaya perlindungan jaringan tersebut diantaranya adalah; meningkatkan kebersihan jaringan internet dari infeksi *malware*, memberikan informasi secara berkala terkait alamat IP berbahaya, *malware*, dan informasi perlindungan jaringan lainnya, mengembangkan prosedur operasi standar sebagai panduan utnuk kerjasama perlindungan jaringan, menilai efektivitas dari informasi yang dibagikan, dengan memberikan umpan balik substantif kepada masing-masing pihak terkait penggunaan informasi tersebut, dan memberikan secara berkala ringkasan dari kerjasama perlindungan jaringan kepada para pelaku utama *cybersecurity.* Selain itu, kedua belah pihak berencana untuk melanjutkan pembahasan mengenai

perlindungan infrastruktur krisis dan asistensi *cybersecurity* dalam pembahasan selanjutnya. Keduanya juga berencana untuk mengadakan diskusi meja bundar yang mempertemukan antara pemerintah China dan AS, bersama dengan perusahaan teknologi untuk berdiskusi mengenai isu-isu yang menjadi persoalan bersama.[249]

Agenda ketiga membahas penyalahgunaan teknologi dan jalur komunikasi dengan tujuan aktivitas terorisme. Seminar dengan agenda yang sama telah terlaksana dengan baik. Keduanya bahkan mempertimbangkan untuk mengadakan seminar kedua yang akan dilaksanakan pada tahun 2017. Keduanya juga sepakat untuk meningkatkan kerjasama dalam hal pertukaran informasi , dan memasukkan agenda perlawanan terhadap aksi terorisme melalui internet maupun aksi dengan tujuan kriminal lainnya.

Mekanisme *hotline* menjadi agenda penutup pada pertemuan ini. Perwakilan China dan AS sepakat untuk melanjutkan mekanisme *cyber hotline* sesuai dengan rencana kerja yang telah dibentuk sebelumnya. Penggunaan *cyber hotline* akan diikuti dengan tinjauan penggunaan secara berkala. Keduanya sepakat untuk tetap menggunakan mekanisme *cyber hotline* sebagai jalur komunikasi khusus antara China dan AS dalam menanggapi peristiwa *cybersecurity.*[250] Terakhir, keduanya sepakat untuk mengadakan dialog selanjutnya pada tahun 2017.

[249] Ibid.
[250] Department of Justice Office of Public Affairs, Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Joint Summary of Outcomes, 2016, < https://www.justice.gov/opa/pr/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues> [accessed 25 September 2018].

5.3.5 *Cyber Agenda* dalam *U.S.-China Law Enforcement and Cybersecurity Dialogue* (LECD)

LECD merupakan wujud kelanjutan dari lima poin kerjasama *cybersecurity* pada tahun 2015, seperti yang telah disebutkan sebelumnya. Terdapat dua agenda yang menjadi fokus dalam dialog LECD. Kedua agenda tersebut adalah kerjasama dalam bidang penegakan hukum, dan *cybersecurity.* Dialog ini merumuskan kerjasama penegakan hukum yang akan dibangun dengan berfokus pada 4 isu yaitu isu-isu mengenai repatriasi, pemberantasan narkotika dan obat-obatan terlarang, perlakuan terhadap buron, *cybercrime* dan *cybersecurity*.[251]

Pada bagian ini, pembahasan akan berfokus pada agenda yang menyangkut isu *cybercrime* dan *cybersecurity.* Keduanya tetap berupaya untuk meningkatkan kerjasama untuk menghadapi *cybercrime.* Upaya yang dilakukan antara lain kerjasama melalui pertukaran informasi kasus *cybercrime* dan permintaan bantuan dalam prosedur MLA. Kasus yang menjadi perhatian meliputi kasus penipuan *cyber* (BEC), peretasan, aktivitas terorisme, dan distribusi pornografi anak melalui internet.[252]

Agenda perlindungan jaringan juga tetap berlanjut dalam kerjasama ini. Begitu juga dengan agenda mekanisme *hotline.* Inisiasi maupun implmenetasi *cyber hotline* dilanjutkan dalam agenda LECD. Keduanya sepakat untuk mempertahankan dan menggunakan mekanisme *hotline* sebagai jalur komunikasi. Mekanisme *hotline* adalah jalur untuk membahas permasalahan mendesak terkait

[251] Ibid.
[252] China Daily, Loc.cit.

cybercrime dan masalah perlindungan jaringan. Pengembangan jalur komunikasi melalui mekanisme *hotline* bertujuan untuk mengembangkan komunikasi antar petinggi negara. Pertemuan selanjutnya dialog LECD diharapkan dapat dilaksanakan kembali pada tahun 2018.

Melalui berbagai penjelasan agenda dalam dialog yang dilakukan oleh China dan AS terkait *cybersecurity*, terlihat bahwa terdapat kontinuitas isu dalam setiap agenda. Isu tersebut turut berkembang sering dengan perkembangan bentuk dialog. Pembahasannya pun beragam, mulai dari agenda yang umum sampai dengan teknis implementasi dari kerjasama *cybersecurity* China dan AS. Akan tetapi, wujud implementasi dari kerjasama tersebut masih belum banyak terlihat dan masih berupa forum dialog *cybersecurity.*

5.3.6 Analisis *cyber issues* melalui *cyber agenda* dalam dialog bilateral China dan AS

Ketika melakukan *cyberdiplomacy*, terdapat beberapa *cyber agenda* yang berada pada isu yang tidak hanya mengenai persoalan keamanan teknis tetapi juga menggambarkan unsur politik. Meskipun terdapat perbedaan jalur diplomatik, yaitu track 1 dan track 1.5, pada umumnya agenda yang diangkat mengacu pada benang merah yang sama. Penelitian ini berupaya menjelaskan isu *cyber* yang menjadi agenda dalam dialog bilateral kerjasama *cybersecurity* China-AS. Melalui berbagai penjelasan *cyber agenda* sebelumnya, terlihat bahwa secara umum terdapat empat *cyber issues* yang diangkat dalam setiap agenda pada saat dilakukannya dialog bilateral. Isu-isu siber tersebut antara lain adalah isu *cybersecurity*, *cybercrime*, *confidence building*, dan *internet governance.*

5.3.6.1 Isu *Cybersecurity*

Isu *cybersecurity* dijelaskan melalui agenda-agenda yang berfokus pada masalah dalam hubungan bilateral *cybersecurity* hingga upaya untuk mencapai kerjasama *cybersecurity* antara China dan AS. Isu *cybersecurity* merupakan isu dominan sekaligus isu yang paling umum dalam agenda *cyberdiplomacy* yang dilakukan oleh China dan AS. Perkembangan dialog yang dilakukan oleh China dan AS pada akhirnya membawa kesepakatan dalam hal kerjasama *cybersecurity.* Agenda yang mengawali adanya isu ini adalah pembahasan terkait permasalahan spionase siber terutama dalam hal pencurian hak kekayaan intelektual.

Dalam forum *cybersecurity dialogue* yang dilakukan oleh CICIR dan CSIS, permasalahan spionase siber tidak mendapatkan banyak penekanan. Permasalahan *cybersecurity* dalam hubungan bilateral China dan AS mengalami peningkatan pada tahun 2013. Sebelumnya, isu *cybersecurity* kerap kali dibahas dalam bentuk agenda mengenai perilaku *cyberspace,* norma *cyberspace.* Agenda dalam dialog tersebut kemudian mulai banyak membahas berbagai langkah yang dapat diambil untuk meningkatkan kerjasama *cybersecurity.*

Forum dialog CWG dibentuk atas prakarsa pada pertemuan Sunnyland Summit. Agenda dalam CWG itu sendiri berfokus pada *cybersecurity* dan permasalahan EMCE. Terlihat adanya upaya untuk mencapai kesepakatan mengenai masalah *cybersecurity*, meskipun permasalahan spionase siber masih tetap ada. Dengan begitu, dapat dilihat bahwa setelah diadakannya Sunnyland Summit, dialog yang dilakukan oleh China dan AS tidak lagi hanya sebatas *confidence building*, tetapi telah mencakup upaya teknis kerjasama *cybersecurity*.

Lalu, diesepakatinya *US-China Cyber Agreement 2015* membawa EMCE menjadi aturan yang berlaku dalam *cyberspace.* Kerjasama tersebut mengawali kesepakatan EMCE lainnya, seperti kesepakatan *cybersecurity* yang tercapai antara China dan Australia pada tahun 2017. Sedangkan *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues* memperlihatkan agenda-agenda didalamnya lebih mengarah pada kerjasama teknis terkait isu *cybersecurity.*

Terdapat tiga bentuk kerjasama yang secara konsisten menjadi agenda dalam *cyberdiplomacy* yang dilakukan oleh China terhadap AS. Pertama adalah peningkatan *cybersecurity* bersama melalui peningkatan keamanan jaringan, bantuan investigasi, dan melakukan simulasi dan upaya penanganan kasus *cybercrime.* Selain itu, kerjasama dilakukan dalam bentuk mekanisme *cyber hotline* dan kerjasama dalam bidang penegakan hukum. Ketiga bentuk upaya kerjasama tersebut juga menjadi poin-poin kesepakatan tersendiri dalam *US-China Cyber Agreement 2015.* Hanya saja, mekanisme *cyber hotline* dan kerjasama dalam bidang penegakan hukum telah lebih dulu menjadi agenda dalam awal pertemuan *cyberdiplomacy* China dan AS.

Pembentukan *cyber hotline* telah menjadi agenda sejak forum CWG. Agenda tersebut kemudian menjadi salah satu poin dalam kerjasama cybersecurity China dan AS pada tahun 2015. Sebagai bentuk kelanjutannya, agenda *cyber hotline* berkembang melalui tiga pertemuan dari dalam dialog *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues,* dan berlanjut hingga LECD. Agenda mengenai *cyber hotline* tidak hanya sebatas komitmen untuk mengembangkan jalur komunikasi, tetapi telah sampai pada pembentukan mekanisme *hotline itu* sendiri

dalam pembahasan terkahirnya. Bahkan, saat ini *cyber hotline* tersebut sudah dapat digunakan oleh kedua negara, terhitung sejak bulan Agustus tahun 2016. *Hotline* tersebut telah secara resmi mulai digunakan pertama kalinya oleh Chen Zhimin, wakil dari Menteri Keamanan Publik China untuk menghubungi Suzanne E. Spaulding, seorang wakil dari Departemen Keamanan Dalam Negeri AS. Keduanya membicarakan capaian kerjasama dalam hubungan *cybersecurity* kedua negara, dan kelanjutan perihal rencana kerjasama dalam bidang penegakan hukum.[253]

Sedangkan bentuk kerjasama dalam bidang hukum telah menjadi agenda sejak pada pertemuan keempat dan keenam *US-China Cybersecurity Dialogue.* Tetapi pembahasan mengenai agenda tersebut tidak mendapatkan kelanjutan yang signifikan hingga forum dialog *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues.* Melalui penegakan hukum bersama, keduanya berupaya untuk memahami hukum yang berlaku di negara masing-masing untuk menghadapi kasus cybercrime. Meskipun masih dalam sebatas pada area prioritas *cybercrime*, agenda kerjasama dalam bidang penegakan hukum dibahas secara lebih lanjut mengenai proses dan prosedur pelaksanaannya.[254] Fokus terhadap kerjasama penegakan hukum menjadi sebuah kerangka kerjasama yang lebih signifikan dalam LECD. Keduanya sepakat untuk mengembangkan penegakan hukum bersama dengan isu strategis lainnya.

[253] CAC, *China-US High-level Joint Dialogue Hotline for Combating Cybercrime and Related Matters*, 2016, <http://www.cac.gov.cn/2016-08/28/c_1119466923.htm> [accessed 25 September 2018],
[254] U.S. Department of Justice, *Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*, Loc.cit.

5.3.6.2 Isu *Cybercrime*

Isu *cybercrime* terlihat dari agenda pembahasan jenis-jenis kejahatan *cyber,* dan fokus prioritas terhadap bentuk *cybercrime* maupun *cyber-enabled crime. Cybercrime* telah menjadi agenda sejak *US China cybersecurity Dialogue*. Dalam dialog tersebut, China dan AS membahas kerjasama dalam mengantisipasi *cybercrime*, tetapi masih dalam tahap mendiskusikan institusi yang kemudian dapat dengan adil menindaklanjuti kasus *cybercrime.* Isu *cybercrime* lalu berkembang menjadi aktivitas illegal yang disebut dengan *cyber-enabled crime.* Beberapa isu *cyber-enabled crime* yang menjadi area prioritas dalam kerjasama bidang penegakan hukum kedua negara antara lain; pencurian hak kekayaan intelektual, penipuan *cyber,* dan kasus pornografi anak. Selain itu, agenda dalam CWG mulai memasukkan perlawanan terhadap terrorisme, meskipun masih belum secara spesifik dalam hal langkah antisipasinya.

Setelah mencapai kerjasama tahun 2015, isu *cybercrime* berkembang menjadi kerangka kerjasama dalam hubungan *cybersecurity* China dan AS. EMCE telah disepakati sebagai aktivitas illegal dan keduanya menyatakan untuk saling berkomitmen dalam memenuhi kesepakatan tersebut.[255] Kemudian, *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues* memperlihatkan peningkatan dalam upaya-upaya teknis untuk menghadapi isu *cybercrime.* Yang sangat terlihat dari dialog ini adalah perkembangan upaya-upaya teknis untuk menghadapi isu *cybercrime*, terutama dalam hal antisipasi *cybercrime* berdasarkan

[255] The Ministry of Foreign Affairs of the People's Republic of China, *Full Text: Outcome list of President Xi Jinping's state visit to the United States,* Loc.cit.

isu prioritas. Selain ketiga kasus yang telah disebutkan, kasus penyalahgunaan internet untuk tujuan terorisme dan perdagangan senjata api *online* masuk sebagai kategori kasus prioritas. Agenda kasus prioritas *cyber-enabled crime* tersebut disebutkan kembali dalam LECD dan menjadi bagian dari mekanisme kerjasama dalam bidang penegakan hukum.

China dan AS telah memperlihatkan adanya kemajuan dalam kerjasama penegakan hukum bersama untuk menghadapi *cybercrime.* Hal ini diperlihatkan oleh keberhasilan koordinasi tim investigasi China dan AS dalam menangkap tersangka pemilik situs pornografi anak. Salah satunya adalah kasus penangkapan Sun Mou dan Huang, warga negara China yang diduga melakukan pelecehan seksual terhadap anak-anak secara *online.* Keberhasilan kepolisian China mendapatkan bantuan oleh petunjuk yang diberikan oleh kepolisian AS yang akhirnya mengantar penyelidikan hingga penangkapan kasus tersebut.[256]

5.3.6.3 Isu *Confidence Building*

Isu *confidence building* menggambarkan upaya kedua negara untuk saling meningkatkan kepercayaannya dalam *cyberspace.* Hal tersebut dilakukan agar permasalahan *cybersecurity* antara keduanya tidak berkembang menjadi masalah yang lebih besar. Peningkatan kepercayaan dilakukan dengan keterbukaan dalam pandangan mengenai prinsip dasar *cybersecurity* masing-masing pihak. Melalui

[256] Xing Bingyin, & Zeng Yaqing, 'China and the United States have twice discussed the fight against cybercrime in the past six months and arrested 17 suspects involved in child pornography', *The Paper*, 2016, <https://www.thepaper.cn/newsDetail_forward_1482997?utm_content=buffercefb3&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer> [accessed 1 October 2018].

perspektif tersebut kemudian diketahui prinsip, norma, dan perilaku yang dianggap pantas maupun tidak pantas dalam *cyberspace* oleh keduanya.

Agenda mengenai *confidence building* diawali pada saat *US-China Cybersecurity Dialogue.* Forum tersebut lebih banyak membahas mengenai isu transparansi dalam kebijakan *cybersecurity.* Sedangkan agenda *confidence building* telah diangkat dalam 4 kali pertemuan. Dalam *joint statement* tahun 2012, kedua pihak representasi juga menyepakati bahwa upaya *confidence building* memang dibutuhkan dalam hubungan *cybersecurity* China dan AS.

Selanjutnya, isu *confidence building* tidak lagi menjadi sebuah agenda dalam pertemuan-pertemuan dialog *cybersecurity* yang dilakukan oleh China dan AS. *Confidence building* lebih diwujudkan melalui upaya-upaya yang dilakukan dalam bentuk sikap yang diambil oleh keduanya. Salah satu bentuk *confidence building* yang dilakukan oleh China adalah pengiriman mentri luar Negeri untuk mengunjungi Washington. Setelah melakukan pengiriman delegasi, presiden Xi Jinping melakukan kunjungan ke AS. Pada saat itu China dan AS mencapai kerjasama *cybersecurity* pada Septembet 2015.

5.3.6.4 Isu *Cyber Governance*

Isu *cyber governance* atau tata kelola internet terlihat dari upaya keduanya untuk mengatur norma *cyberspace* secara internasional. Agenda tata kelola internet termasuk sebagai agenda yang dibahas dalam *U.S.-China Cyber Security Dialogue.* Pembahasan dalam agenda tersebut masih pada seputar isu-isu *cyber governance* secara umum, seperti halnya pembahasan mengenai perkembangan isu tata kelola internet pada saat ini. Selanjutnya, China dan AS melanjutkan pembahasan

mengenai tata kelola internet dalam CWG. Keduanya sepakat untuk meningkatkan dialog terkait pembentukan norma dan prinsip dalam *cyberspace.* Hal tersebut memperlihatkan bahwa agenda mengenai tata kelola internet juga menjadi pembahasan dalam dialog track 1, dimana dialog dilakukan oleh perwakilan resmi pemerintah.

Tetapi, agenda tata kelola internet tidak mendapatkan banyak sorotan dalam forum-forum selanjutnya. isu mengenai tata kelola internet tidak menjadi sebuah agenda khusus, dan hanya dilakukan penekanan terhadap upaya yang telah disebutkan dalam *US-China Cyber Agreement 2015*. Disebutkan bahwa kedua belah pihak dilarang untuk mendukung aktivitas EMCE dan berkomitmen dalam mengidentifikasi dan mengembangkan norma perilaku negara dalam *cyberspace*.[257] Agenda tata kelola internet tidak menjadi agenda dalam forum dialog *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues.* Sedangkan dalam LECD, Meskipun tidak menjadi sebuah agenda, dibawanya isu tata kelola internet telah menunjukkan adanya komitmen keduanya untuk bekerjasama dalam membangun tata kelola internet.

Forum dialog bilateral yang telah dijelaskan diatas menggambarkan isu cyber merupakan isu yang kompleks dan sensitif tetapi juga penting dalam hubungan bilateral China dan AS. Meskipun dalam bentuk yang berubah-ubah, dialog bilateral berhasil dipertahankan pada saat sebelum dan setelah terbentuknya kerjasama *cybersecurity*. Isu *cyber* dalam hubungan bilateral China dan AS telah banyak mengalami perubahan. Hal ini menunjukkan adanya perkembangan dalam

[257] China Daily, Loc.cit.

agenda dialog yang dilakukan China dan AS, turut membawa perkembangan dalam agenda pembahasan isu *cyber*.

Keduanya berhasil membangun sebuah kerangka kerjasama yang tidak hanya sebatas di permukaan saja tanpa adanya bentuk implementasi teknis atas kesepakatan tahun 2015. Hal ini menunjukkan bahwa keduanya masih berupaya untuk menjaga stabilitas dalam hubungan cybersecurity. Permasalahan dalam norma internasional masih berada dalam perdebatan keduanya. Tetapi, disamping perbedaan prinsip dan pandangan terkait cybersecurity, dialog bilateral yang dilakukan oleh China dan AS hingga saat ini berhasil mempertahankan hubungan *cybersecurity* mereka tetap berada dalam situasi yang damai.

5.4 Peran Kementerian Luar Negeri China sebagai diplomat dalam *Cyberdiplomacy* China terhadap AS

Pendekatan institusional menjelaskan bagaimana suatu pemerintahan menangani isu *cyber* internasional dalam struktur pemerintahannya, terutama mengenai peran Kementerian Luar Negeri.[258] *Cyberdiplomacy* yang dilakukan China lebih banyak diinisiasi pada saat era pemerintahan presiden Xi Jinping. Pemerintah pusat berperan penting dalam melakukan koordinasi kebijakan dalam keseluruhan struktur pemerintahan. Salah satu bentuk kebijakannya adalah *cyberdiplomacy* dengan AS melalui berbagai dialog bilateral dengan isu *cybersecurity* dan berbagai isu lainnya.

[258] André Barrinha & Thomas Renard, '*Cyber*-diplomacy: the making of an international society in the digital age', *Global Affairs*, (2017), pp. 1-12, (p. 7).

Apabila dilihat berdasarkan pendekatan institusional, China tidak memiliki departemen baru di bawah Kementerian Luar Negeri untuk menangani isu *cyber*. Tetapi, China memiliki sebuah unit koordinasi yang menjadi pusat aktivitas dan segala kebijakan terkait isu *cyber* internasional. Dalam struktur pemerintahan China, terdapat sebuah komisi yang memiliki wewenang sebagai pembuat rekomendasi kebijakan *cyberspace* China, yaitu OCCSIC. OCCSIC berada di bawah mandat Komite Sentral Partai Komunis Cina atau *Central Committee of the Communist Party of China* (CCCPC), dan dikepalai oleh presiden Xi Jinping.[259]

Salah satu kementerian yang menjadi bagian dari OCCSIC adalah Kementerian Luar Negeri China. Hal tersebut menggambarkan bahwa kementerian tersebut hanya menjadi bagian kecil dari OCCSIC.[260] Selain itu, OCCSIC berisi orang-orang yang memiliki posisi penting dalam struktur pemerintahan China, dan juga perwakilan dari setiap kementerian yang bersinggungan dengan kebijakan *cybersecurity*.[261] Hal yang menarik dari struktur pemerintahan China adalah pada dasarnya pola diplomatik dalam pengambilan kebijakan isu *cybersecurity* China terfragmentasi pada beberapa kementerian yang berbeda. Isu *cyber* adalah isu yang selalu berkembang, sehingga setiap departemen berkaitan satu sama lain. Tetapi,

[259] Dengan catatan bahwa *Office of the Central Cyber Security and Informatization Commission* (OCCSIC) merupakan wujud baru dari *Cybersecurity And Informatization Leading Group* (SILG). DIkutip berdasarkan Jon R. Lindsay, 'Introduction', in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, (eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, (Oxford University Press, 2015), pp. 13-14.
[260] Ibid.
[261] Mark A. Stokes, 'The Chinese People's Liberation Army Computer Network Operations Infrastructure', Op. cit., p. 164.

pengambilan kebijakan tetap saja tersentralisasi pada OCCSIC, terutama pada pemimpin negara yaitu Xi Jinping.[262]

5.4.1 Diplomat China dalam dialog bilateral *cybersecurity* China-AS

Pada bagian ini, fokus penelitian terletak pada peran perwakilan negara dalam *cyberdiplomacy* yang dilakukan oleh China. *U.S-China. Cybersecurity Dialogue* diselenggarakan oleh CICIR dan CSIS, dimana keduanya merupakan *think tanks* yang berfokus pada studi internasional. *China Institute of Contemporary International Relations* (CICIR) sebagai perwakilan dari China dan *Center for Strategic and International Studies* (CSIS) sebagai perwakilan dari AS. Hanya saja, pertemuan ini bersifat rahasia sehingga informasi yang didapatkan mengenai peran diplomat dalam dialog ini terbatas. Analisis yang kemudian dapat dilakukan adalah melalui agenda atas dialog yang dilakukan oleh keduanya.

Situs resmi CSIS tidak menjelaskan secara rinci perwakilan dari pihak China maupun AS dalam setiap pertemuan. Tetapi, terdapat dua buah artikel didalamnya, yang menjelaskan pertemuan keempat dan kesembilan dari dialog tersebut. Pada pertemuan keempat dan kesembilan, delegasi yang mewakili negara China kurang lebih sama. Mereka adalah representasi dari pihak CICIR, dan beberapa perwakilan dari pemerintah. Terdapat representasi negara China yang berasal dari Kementerian Luar Negeri, PLA, Kementerian Industri dan Teknologi Informasi, dan Kementerian Keamanan Publik.[263]

[262] Jean-Pierre Cabestan, 'China's Institutional Changes in the Foreign and Security Policy Realm Under Xi Jinping: Power Concentration vs. Fragmentation Without Institutionalization', *East Asia* 34, (springer, 2017), pp. 113–131.
[263] Lewis, Loc.cit.

Sedangkan perbedaannya adalah pada pertemuan kesembilan, China secara khusus mengirimkan CN-CERT yang merupakan bagian dari Kementerian Industri dan Teknologi Informasi, dan juga perwakilan dari Kantor Informasi Dewan Negara.[264] Representasi China pada pertemuan kesepuluh masih sama dengan pertemuan kesembilan. Hanya saja, tidak ada lagi delegasi yang berasal dari Kantor Informasi Dewan Negara China. Posisi tersebut digantikan oleh *The Cyberspace Administration of China* (CAC). Sedangkan PLA digantikan oleh delegasi yang berasal dari Kementerian Pertahanan Republik Rakyat China.[265] Melalui *US-China cybersecurity dialogue*, representasi negara China berperan untuk mengguangkan *cyber sovereignty* sebagai nilai dan prinsip dasar *cyberspace* dan mencegah hegemoni dalam *cyberspace*. Hal tersebut selaras dengan kepentingan nasional China yang dijelaskan dalam dokumen strategi kerjasama internasional.

Dialog selanjutnya adalah CWG, yang menjadi rangkaian pertemuan S&ED kelima. Seperti yang telah dijelaskan sebelumnya, CWG digunakan untuk melanjutkan diskusi mengenai isu *cybersecurity* sebagai kelanjutan pertemuan Sunnyland Summit. Pada saat CWG berlangsung, hadir representasi negara pada saat itu diantaranya adalah perwakilan dari Kementerian Luar Negeri, Kementerian Pertahanan, Kementerian Keamanan Publik, Kementerian Industri dan Teknologi

[264] The Center for Strategic and International Studies (CSIS), *9th Meeting of the CSIS-CICIR Cybersecurity Dialogue*, n.d., <https://www.csis.org/events/9th-meeting-csis-cicir-cybersecurity-dialogue[accessed 3 October 2018].

[265] Michael Sulmeyer, dan Amy Chang, merupakan partisipan dalam *U.S. Cybersecurity Dialogue* pada pertemuan kesepuluh. Mereka adalah delegasi AS yang berafiliasi dengan kelompok peneliti studi internasional *The Belfer Center for Science and International Affairs.* Informasi mengenai partisipan China diceritakan oleh keduanya melalui Michael Sulmeyer, Amy Chang Three Observations on China's Approach to State Action in Cyberspace, 2017, <https://www.lawfareblog.com/three-observations-chinas-approach-state-action-cyberspace> [accessed 3 October 2018].

Informasi, Kementerian Perdagangan, dan Kantor Informasi Dewan Negara.[266] Selanjutnya, pertemuan kelima dialog S&ED dipimpin oleh Menteri Luar Negeri Republik Rakyat China, Yang Jiechi, sebagai representasi dari presiden Xi Jinping, dan Menteri Luar Negeri Amerika Serikat, John Kerry sebagai representasi dari presiden Barack Obama.[267]

Meskipun CWG terhenti, isu *cybersecurity* dalam hubungan kedua negara mencapai sebuah titik temu pada tahun 2015. Sebelumnya, China mengirimkan seorang Ketua Komisi Urusan Politik dan Hukum Pusat Partai Komunis China, Meng Jianzhou, sebagai diplomat China.[268] Tujuannya adalah untuk meluruskan permasalahan terkait isu *cyber* yang dihadapi oleh kedua negara. Pada kunjungan tersebut, Meng Jianzhou kembali memberikan penekanan terkait posisi China yang menentang aktivitas pencurian hak kekayaan intelektual dan rahasia bisnis. Pada September 2015, presiden Xi Jinping dan Barack Obama berhasil mencapai kerjasama *US-China Cyber Agreement 2015.* Disini, presiden Xi Jinping lebih memilih Meng, seorang Menteri Keamanan Publik yang juga seorang konsilor negara dibandingkan dengan mengirimkan seorang Menteri Luar Negeri, dimana peran tersebut idealnya merupakan peran dari seorang Menteri Luar Negeri.[269]

---

[266] U.S. Department of Justice, *Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*, Loc.cit.
[267] Embassy of the People's Republic of China in the United States of America, *U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track*, Loc.cit.
[268] South China Morning Post, *China seeks to ease Sino-US cyber tensions with top-level talks ahead of Xi Jinping's US trip*, 2015, <https://www.scmp.com/news/china/diplomacy-defence/article/1857903/china-seeks-ease-sino-us-cyber-tensions-top-level-talks> [accessed 4 October 2018].
[269] Rogier Creemers, Paul Triolo, Samm Sacks, Xiaomeng Lu, and Graham Webster, 'China's Cyberspace Authorities Set to Gain Clout in Reorganization', *New America*, 2018, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/> [accessed 4 October 2018].

Pada tiga pertemuan *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*, perwakilan negara China yang memimpin dialog tersebut adalah Dewan Negara China, yaitu Guo Shengkun, bersama dengan perwakilan dari AS yaitu Jaksa Agung Loretta E. Lynch, dan Sekretaris Departemen Keamanan Dalam Negeri, Jeh Johnson.[270] Representasi negara China lainnya, berasal dari Komisi Urusan Politik dan Hukum Pusat Partai Komunis China, Kementerian Keamanan Publik, Kementerian Luar Negeri, Kementerian Industri dan Teknologi Informasi, Kementerian Keamanan Nasional, Mahkamah Agung, dan Kantor Informasi Dewan Negara.

Sebelum memasuki pertemuan kedua, Wang Yi, Menteri Luar Negeri China, melakukan perjalanan ke Washington untuk menunjukkan niatan baik China yang hendak meningkatkan hubungannya dengan AS melalui kerjasama. Wang Yi melakukan konferensi pers bersama dengan John Kerry, Menteri Luar Negeri AS. Pada saat itu, Wang Yi mengungkapkan harapan China untuk dapat saling terjalin kepercayaan diantara China dan AS, begitu juga dengan hasil yang positif dari dialog-dialog antara China dan AS, salah satunya adalah dialog tingkat tinggi *cybercrime* dan isu terkait.[271]

Pada pertemuan ketiga, dialog dihadiri oleh representasi negara China yang berasal dari Kementerian Keamanan Publik, CAC, Kementerian Luar Negeri, Kementerian Industri dan Teknologi Informasi, Kementerian Keamanan Nasional,

[270] The State Council of People's Republic of China, *China, US to jointly fight cyber crime,* 2016, <http://english.gov.cn/state_council/state_councilors/2016/06/15/content_281475372216337.htm> [accessed 4 October 2018].
[271] U.S. Department of State, *Remarks With Chinese Foreign Minister Wang Yi*, 2016, <https://2009-2017.state.gov/secretary/remarks/2016/02/253164.htm> [accessed 5 October 2018].

dan Mahkamah Agung.[272] Sedangkan pada saat dialog LECD, Guo Shengkun kembali ditunjuk untuk memimpin jalannya dialog tersebut.[273] Selain seorang dewan negara, beliau juga merupakan seorang Menteri Keamanan Publik Republik Rakyat China. Disini, tidak terlihat adanya peran penting yang dimiliki oleh perwakilan Kementerian Luar Negeri.

Melalui penjelasan representasi negara terlihat bahwa meskipun China memiliki unit koordinasi yang menangani isu *cybersecurity*, tetapi tidak ada kesatuan langkah yang jelas bagi para perwakilan diplomatik yang dikirm sebagai diplomat China. Hal ini terlihat dari perubahan diplomat China dalam negosiasi bilateral mengenai kerjasama *cybersecurity* dengan AS. Karena *cybersecurity* adalah sebuah isu yang dapat bersinggunggan dengan isu lainnya, maka diplomat yang dikirim sebagai representasi negara pun berasal dari Kementerian yang berbeda-beda. Tetapi, karena dalam struktur pemerintahan China yang memegan kendali sebagai pembuat kebijakan adalah para konsilor negara, maka merekalah yang banyak memiliki peran sebagai perwakilan negara dalam hubungan luar negeri China, termasuk juga dalam hubungan *cybersecurity* China dan AS.

Kerjasama *cybersecurity* menjadi tujuan kepentingan nasional China berdasarkan strategi kerjasama *cybersecurity* internasional China. Dokumen tersebut merupakan buah dari rekomendasi kebijakan yang dikeluarkan oleh CAC,

---

[272] Chen Weihua, China, US to do more on cyber crime, *China Daily*, 2016, <http://usa.chinadaily.com.cn/a/201612/08/WS5a30d69da3108bc8c672f523.html> [accessed 5 October 2018].

[273] Ministry of Foreign Affairs, the People's Republic of China, *Guo Shengkun to Travel to the United States to Co-Chair the First Round of China-US* Law Enforcement and Cyber Security Dialogue,
2017, <https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/wsrc_665395/t1499253.shtml> [accessed 6 October 2018].

sebuah badan administratif *cyberspace* yang berada di bawah OCCSIC. Didalamnya ditekankan bahwa China mengutamakan perdamaian sebelum kedaulatan. Hal tersebut dapat berarti sebelum mencapai kedaulatan, China terlebih dahulu meningkatkan kerjasama dalam hubungan *cybersecurity* nya dan mencegah perlombaan senjata dalam *cyberspace.*[274]

Pada saat pembentukan OCCSIC pun, dalam pidatonya, Xi Jinping mengatakan bahwa ia akan menjadikan China sebagai negara dengan kekuatan *cyber*. Pemerintahannya akan menjadikan *cybersecurity* sebagai keamanan nasional. Untuk mewujudkan ambisinya, disebutkan bahwa China akan meningkatkan pengembangan teknologi dan meningkatkan kerjasama *cybersecurity* dengan negara lainnya.[275] Salah satu caranya yaitu menjadikan China sebagai negara yang memiliki *cyber sovereignty*. Alat diplomatik kemudian digunakan untuk mewujudkan ambisinya melalui kerjasama *cybersecurity.*[276] Hingga dalam kurun waktu dekat ini, niatan tersebut masih ditunjukkan oleh Menteri Luar Negeri Yang Jiechi. Ia mengatakan dalam pidatonya bahwa China akan tetap mengejar kepentingan nasional, melindungi kedaulatan, dan mendorong kerjasama dalam melawan terorisme, *cyberspace,* dan dalam bidang penegakan hukum.[277]

---

[274] Adam Segal, 'Chinese Cyber Diplomacy in a New Era of Uncertainty', Op.cit., p. 3.
[275] The Cyberspace Administration of China, *The first meeting of the Central Network Security and Informatization Leading Group held an important speech by Xi Jinping,* 2014, <http://www.cac.gov.cn/2014-02/27/c_133148354.htm> [accessed 16 October 2018].
[276] Central Information Office network theory study group, *In-depth implementation of General Secretary Xi Jinping's strategic thinking of network power, solidly promote network security and informationization,* 2017, <http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm> [accessed 24 October 2018].
[277] The Ministry of Foreign Affairs of the People's Republic of China, *Study and Implement General Secretary Xi Jinping's Thought on Diplomacy in a Deep-going Way and Keep Writing New Chapters of Major-Country Diplomacy*

BAB VI

PENUTUP

6.1 Kesimpulan

Persoalan keamanan baru, seperti halnya ranah *cybersecurity*, dapat menimbulkan potensi persaingan antar negara untuk menguasai ranah tersebut. Begitu juga dengan kerjasama. Dalam *cyberspace*, China dan AS pun memiliki kepentingannya masing-masing. Keduanya kemudian dapat mencapai kesepakatan dan kerjasama dalam ranah *cybersecurity.* Kerjasama tersebut tidak terjadi dalam waktu semalam saja. Terdapat sebuah proses berkelanjutan yang pada akhirnya mengantar kedua negara membentuk sebuah kerangka kerjasama untuk menangani permasalahan *cybersecurity* dalam hubungan bilateral kedua negara.

Alur penelitian *cyberdiplomacy* dalam penelitian ini melihat bagaimana kerjasama China-AS dalam *cybersecurity*. *Cyberdiplomacy* yang dilakukan oleh China pertama dapat dilihat dari aktivitas diplomatik yang dilakukan oleh China dan AS di bidang *cyber*. Didalamnya, diangkat isu-isu *cyber* yang ada dalam hubungan bilateral kedua negara dan dibawa oleh para representasi negara dalam forum tersebut. Setiap representasi negara tentu membawa kepentingan nasional yang menjadi tujuan, nilai dan prinsip dasar *cyberspace* sebagai pedoman dalam melakukan aktivitas diplomatik.

---

with Distinctive Chinese Features, 2017, <https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1478497.shtml> [accessed 4 November 2018].

Aktivitas diplomatik yang dilakukan oleh China secara bilateral dengan AS adalah melalui dialog dan pertemuan bilateral antara perwakilan kedua negara. Dialog tersebut terbagi menjadi dua bentuk, yaitu dialog track 1 dan track 1.5. Sebelum tercapainya kesepakatan cybersecurity antara China dan AS, keduanya berupaya untuk menyamakan pandangan dalam *US-China Cybersecurity Dialogue.* Jalur dialog resmi antar pemerintah pertama untuk membahas persoalan *cybersecurity* adalah *U.S.-China Strategic and Economic Dialogue.* Didalamnya terdapat sebuah *cyber working group,* sebuah *working group* yang dikhususkan untuk membahas permasalahan *cyberspace* kedua negara.

Kerjasama *cybersecurity* China dan AS baru mencapai kesepakatan pada saat presiden Xi Jinping melakukan kunjungan kenegaraan ke Amerika Serikat. Kedua belah pihak sepakat untuk tidak melakukan aktivitas EMCE terhadap satu sama lain. Implementasi dari kerjasama tersebut berupaya untuk diwujudkan melalui forum dialog *U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues.* Pada akhirnya isu cybersecurity dalam hubungan bilateral China dan AS tergabung dalam kerangka kerjasama yang lebih signifikan yaitu *U.S.-China Law Enforcement and Cybersecurity Dialogue*.

Terlihat adanya beberapa isu siber yang menjadi agenda didalam aktivitas *cyberdiplomacy* yang dilakukan oleh China. Isu-isu siber tersebut antara lain adalah isu *cybersecurity, cybercrime, confidence building,* dan *internet governance.* Setiap isu memiliki penekanan yang berbeda-beda. Tetapi, isu yang paling mendominasi didalamnya adalah isu *cybersecurity.*

Apabila menjelaskan aktor yang membawa kepentingan nasional China saat melakukan *cyberdiplomacy,* Kementerian Luar Negeri China menjadi sorotan utama. Akan tetapi, China memiliki cara yang berbeda dengan negara lainnya dalam menangani isu *cyber* internasional. Berdasarkan pendekatan institusional, China tidak memiliki departemen baru di bawah Kementerian Luar Negeri untuk menangani isu *cyber*. Tetapi, China memiliki sebuah unit koordinasi yang menjadi pusat aktivitas dan segala kebijakan terkait isu *cyber* internasional. Peran tersebut dimiliki oleh *Office of the Central Cyber Security and Informatization Commission* (OCCSIC).

Setiap representasi negara bertanggung jawab untuk membawa kepentingan nasional negaranya. *International Strategy of Cooperation on Cyberspace* menggambarkan bagaimana *cyber sovereignty* merupakan prinsip dasar dalam setiap kerjasama *cybersecurity* yang dilakukan oleh China. China dan AS memiliki pandangan berbeda terkait nilai kedaulatan. Tetapi, pada saat melakukan *cyberdiplomacy* dengan AS, China terus mendorong nilai *cyber sovereignty* didalamnya.

Adanya kelanjutan upaya China untuk melanjutkan dialog dan diskusi terkait *cybersecurity* sebelum maupun sesudah tercapainya kerjasama menunjukkan antusiasme yang dimiliki China amatlah tinggi. Terlihat adanya perkembangan dalam bentuk dan isi dari setiap mekanisme dialog tingkat tinggi untuk menyelesaikan permasalahan *cybersecurity* antara China dan AS. Tetapi di sisi lain, kesepakatan yang tercapai antara keduanya masih terlalu luas dan tidak menjelaskan aturan kerjasama secara spesifik. Tidak ada penjelasan mengenai

hukuman bagi yang melanggar isi dari kerjasama tersebut. Selain itu, perjanjian tersebut juga tidak terdapat aturan mengenai aktivitas spionase dengan motif non-komersial. Penulis berpendapat bahwa China masih bermain aman dalam merumuskan kerjasamanya dengan AS. China tidak dirugikan dalam kerjasama tersebut. Sebagai pihak yang seringkali mendapatkan tuduhan, menyepakati sebuah kerjasama adalah cara yang digunakan China untuk menunjukkan kesungguhannya dalam menyelesaikan permasalahannya dengan AS. Meskipun dalam implementasinya, penyelesaian dari masalah *cybersecurity* tersebut masih belum menemukan titik penyelesaian, mengingat bahwa identifikasi pelaku dari aktivitas dalam *cyberspace* adalah hal yang sangat sulit.

Keputusan China untuk menyepakati kerjasama dengan AS menjadi salah satu strategi China untuk membawa mendorong nilai *cyber sovereignty* dalam kancah internasional. Meskipun *cyber sovereignty* belum disepakati sebagai nilai dalam tata kelola internet secara internasional, tetapi dengan tercapainya kerjasama antara China dan AS di bidang *cybersecurity* maka China memiliki kewenangan untuk mengatur hukumnya sendiri terkait aktivitas EMCE.

Melalui kerjasama dan konsep *cyber sovereignty*, China melancarkan apa yang menjadi kebijakan domestik, sebuah tujuan domestik dan juga sebuah tujuan politik luar negeri China itu sendiri. Pertama, melalui kerjasama, China memiliki kewenangan untuk meningkatkan *cybersecurity* yang ada di wilayah domestiknya. Karena seperti yang telah dijelaskan sebelumnya bahwa, secara domestik China adalah negara dengan tingkat pengawasan dan kontrol terhadap *cybersecurity* yang tinggi. Secara internasional, China berupaya untuk mewujudkan politik luar

negerinya yaitu "*New Type of Major Power Relations*", dan *"a cyberspace community of common destiny".* Kedua bentuk hubungan tersebut diwujudkan China melalui kerjasama *cyberspace* antara China dan AS, dimana kerjasama tersebut menjadi awal dari kerjasama China dengan negara lainnya dalam ranah *cybersecurity.*

6.2 Saran

Permasalahan *cybersecurity* sebagai objek penelitian merupakan hal yang baru dalam studi hubungan internasional. Hal ini juga banyak dibuktikan oleh minimnya peneliti hubungan internasional yang mengangkat *cybersecurity*. Kompleksitas ranah *cybersecurity* memiliki tantangan tersendiri sebagai objek penelitian. *Cybersecurity* dapat dihubungkan dengan kebijakan, strategi diplomasi, ranah pertahanan dan keamanan, dan sebagainya. Untuk itu, peneliti harus dapat menentukan fokus penelitian yang spesifik dalam ranah *cybersecurity*, karena kecenderungan untuk menulis hal-hal diluar lingkup penelitian sangat tinggi. Terlebih lagi, *cybersecurity* memiliki sifat alami yang juga tidak kalah kompleks. Hal ini berkaitan dengan atribusi pelaku, *deterrence*, dan hal-hal yang berkaitan lainnya.

Cyberdiplomacy juga merupakan ranah baru dalam hubuungan internasional. Ilmu dan diskursi *cyberdiplomacy* masih berkembang, sehingga konsep *cyberdiplomacy* yang digunakan dalam penelitian ini masih sangat prematur. Berbeda dengan penggunaan *cyber* sebagai alat dari diplomasi publik, *cyberdiplomacy* jauh lebih minim penggunaannya. Penjelasan *cyberdiplomacy* itu sendiri masih belum memiliki definisi konseptual secara universal.

Penulis menyadari masih banyak kekurangan dalam penelitian ini, mulai dari yang bersifat substansial maupun dari segi penulisan. Penulis menyarankan bagi penelitian lain yang hendak mengangkat tema yang sama dengan penulis, untuk menggunakan perspektif yang berbeda dari negara pelaku *cyberdiplomacy* lainnya, seperti kerjasama *cybersecurity* antara Rusia dan AS pada tahun 2013. Apabila hendak mengangkat *cybersecurity* China secara lebih mendalam, penulis menyarankan untuk melihat upaya China untuk menjadi negara dengan kekuatan *cyber* yang salah satu upayanya adalah melalui *cyberdiplomacy*. Meskipun tidak banyak penjelasan konseptual mengenai *cyberdiplomacy,* tetapi wujud praktik dari aktivitas tersebut banyak ditemukan dalam fenomena hubungan internasional. Sehingga hal tersebut tidak menjadi penghalang untuk mengembangkan keilmuan hubungan internasional dan kaitannya dengan *cyberspace.*

DAFTAR PUSTAKA

Abomhara, Mohamed and Køien, Geir M. 'Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks.' *Journal of Cyber Security*. vol. 4. (2015). pp. 65–88.

Austin, Greg. C*ybersecurity in China The Next Wave.* (Springer, 2018).

Barrinha, André, & Renard, Thomas. '*Cyber*-diplomacy: the making of an international society in the digital age'. *Global Affairs.* (2017). pp. 1-12.

Bingyin, Xing & Yaqing, Zeng. 'China and the United States have twice discussed the fight against cybercrime in the past six months and arrested 17 suspects involved in child pornography'. *The Paper.* 2016. <https://www.thepaper.cn/newsDetail_forward_1482997?utm_content=buffercefb3&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer> [accessed 1 October 2018].

Cabestan, Jean-Pierre. 'China's Institutional Changes in the Foreign and Security Policy Realm Under Xi Jinping: Power Concentration vs. Fragmentation Without Institutionalization'. *East Asia* 34. (springer. 2017). pp. 113–131.

Cai, Cuihong. 'Cybersecurity in Chinese Context: Changing Concepts, Vital Interests, and Cooperative Willingness.' (paper presented at 9th Berlin Conference on Asian Security (BCAS), June 14-16, 2015). <https://www.swp-berlin.org/fileadmin/contents/projects/BCAS2015_Cai_Cuihong_Web.pdf> [accessed 11 February 2017].

Carayannis, Elias G., Campbell, David F.J. & Marios, P.E., *Cyber-Development, Cyber-Democracy and Cyber-Defense. (*Springer. 2014).

Center for Strategic and International Studies (CSIS). *Track 1.5 U.S.-China Cyber Security Dialogue,* 2009-2015. <https://www.csis.org/programs/technology-policy-program/cybersecurity-and-governance/other-projects-cybersecurity/track-1> [accessed 19 September 2018].

Central Committee of the Communist Party of China Beijing. *The 13th Five-Year Plan For Economic And Social Development Of The People's Republic Of China (2016–2020).* (2016). China Central Compilation & Translation Press <http://en.ndrc.gov.cn/newsrelease/201612/P020161207645765233498.pdf> [accessed 24 November 2017].

Central Information Office network theory study group. *In-depth implementation of General Secretary Xi Jinping's strategic thinking of network power, solidly promote network security and informationization*. 2017. <http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm> [accessed 24 October 2018].

Chang, Amy & Sulmeyer, Michael. *Three Observations on China's Approach to State Action in Cyberspace.* 2017. <https://www.lawfareblog.com/three-observations-chinas-approach-state-action-cyberspace> [accessed 23 September 2018].

Chang, Amy. *Warring State: China's Cybersecurity Strategy*. (Center for a New American Security. 2014). p. 12.

China Central Television. *China: Hacking allegations "groundless". 2013.* <http://english.cntv.cn/program/newshour/20130220/104023.shtml> [accessed 14 December 2017].

China Daily USA. *US should 'explain hacking activity'.* 2013. <http://usa.chinadaily.com.cn/epaper/2013-06/14/content_16621289.htm> [accessed 14 February 2018].

China Internet Network Information Center (CNNIC). *Statistical Report on Internet Development in China.* 2018. <https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf> [accessed 20 April 2018].

Chua, Joseph B. M. '2015 U.S.-China *Cyber* Agreement: a new hope, or "the empire strikes back"?'. (Monterey. California: Naval Postgraduate School. 2017).

China Military Online. *MND website and China Military Online attacked by overseas hackers 144,000-odd times per month*. 2013. <http://en.people.cn/90786/8151567.html> [accessed 17 July 2018].

China Daily. *Summary of outcomes of First China-US Law Enforcement and Cybersecurity Dialogue.* 2017. <http://www.chinadaily.com.cn/world/2017-10/06/content_32924234.htm> [5 July 2018].

China Institute of Contemporary International Relations (CICIR) and Center for Strategic and International Studies (CSIS). *Bilateral Discussions on Cooperation in Cybersecurity.* 2012. <http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf> [accessed 27 June 2018].

Creemers, Rogier. Triolo, Paul. Sacks, Samm. Lu, Xiaomeng and Webster, Graham. 'China's Cyberspace Authorities Set to Gain Clout in Reorganization'. *New America.* 2018. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/> [accessed 4 October 2018].

Cyber Espionage and the Theft of U.S. Intellectual Property and Technology, Testimony of Larry M. Wortzel before the House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations. 2013. <http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf> [accessed 24 July 2018].

Cyberspace Administration of China Theoretical Studies Center Group. 'In-depth implementation of General Secretary Xi Jinping's network strategy of

strengthening the country and solidly promoting network security and informationization'. *Qiushi.* September 15 2017. <http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm> [accessed 18 September 2018].

Danca, Dana. '*Cyber* Diplomacy — A New Component of Foreign Policy'. *Journal of Law and Administrative Sciences*. Issue 3. (2015). pp. 93–97.

Davila, Juan Manuel De La Torre. 'Cybersecurity and United States-China Relations: A Theoritical Perspective'. (International Master's Program in International Studies National Chengchi University. 2018).

Department of Justice United States of America. *US. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*. 2014 <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-*cyber*-espionage-against-us-corporations-and-labor> [accessed 29 July 2018].

Department of Justice United States of America. *First U.S.-China Law Enforcement and Cybersecurity Dialogue Summary of Outcomes.* Available from: <https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue> [25 December 2017].

Denmark, Abraham M. 'US Strategic Rebalancing and China's Rise', in Mingjiang Li & Kalyan M. Kemburi (Ed.). *New Dynamics in US–China Relations* (Routledge. 2015).

Dingding, Chen. 'Shaping the future of Sino-American Relations Power Shift and Strategic Rivalry', in Mingjiang Li & Kalyan M. Kemburi (Ed.). *New Dynamics in US–China Relations* (Routledge. 2015).

Directorate-General for External Policies European union. *China's foreign policy and external relations*. (2015).

DR. Lexy Moleong, M.A., *Metodologi Penelitian Kualitatif.* Bandung: PT Remaha Rosdakarya. 2006.

Embassy of the People's Republic of China in the Republic of Kenya. *The Third China-U.S. Strategic Security Dialogue Held in Washington, D.C.*. 2013. <http://ke.china-embassy.org/eng/zgyw/t1058060.htm> [accessed 29 June 2018].

Embassy of the People's Republic of China in the United States of America. *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 13.* 2013 < http://www.china-embassy.org/eng/fyrth/t1050375.htm> [accessed 14 July 2018].

Embassy of the People's Republic of China in the United States of America. *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on June 28.* 2013 <https://www.fmprc.gov.cn/ce/cebn/eng/fyrth/t1054303.htm> [accessed 14 July 2018].

Embassy of the People's Republic of China in the United States of America. *Foreign Ministry Spokesperson Liu Weimin's Regular Press Conference on December 12, 2011*. 2011. <http://www.china-embassy.org/eng/fyrth/t887523.htm> [accessed 26 July 2018].

Embassy of the People's Republic of China in the United States of America. *Full text of Hu Jintao's report at 18th Party Congress*. 2012. <http://www.china-embassy.org/eng/zt/18th_CPC_National_Congress_Eng/t992917.htm> [accessed 29 February 2017].

Embassy of the People's Republic of China in the United States of America. *U.S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track.* 2013. <http://www.china-embassy.org/eng/zmgxss/t1058593.htm> [accessed 29 June 2018].

Fire Eye. *APT1 Exposing One of China's Cyber Espionage Units.* 2013. <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> [accessed 15 November 2017].

Fire Eye. *Redline Drawn: China Recalculates its use of Cyber Espionage*. 2016. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-chinaespionage.pdf [accessed 30 July 2018].

General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *UN document A/65/201*. 2010. < http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf> [accessed 16 February 2018].

General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *UN document A/68/98.* 2013. <www . un . org / ga / search / view _ doc . asp ? symbol= A / 68 / 98&referer= / english / &Lang= E> [accessed 5 July 2018].

Gerridge, B. R. *Diplomacy: Theory and Practice* . Fourth Edition. (Palgrave : Hampshire : 2009).

Harold, Scott Warren. Libicki, Martin C., Cevallos, Astrid Stuth. *Getting to Yes with China in Cyberspace*. <http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf> [accessed 27 September 2018].

Heinl, Caitríona H. 'New Trends in Chinese Foreign Policy: The Evolving Role of Cyber'. *Asian Security*. (2017).

Hitchens, Theresa & Goren, Nilsu. *International Cybersecurity Information Sharing Agreements*. (Center For International and Security Studies at Maryland. 2017).

Hollis, Duncan B. *China and the US Strategic Construction of Cybernorms: The Process Is the Product.* Hoover Working Group on National Security, Technology, and Law, Aegis Paper Series No. 1704 (2017).

Horwitz, Josh. 'Tim Cook and Sundar Pichai's surprise remarks at China's "open internet" conference'. Quartz. <https://qz.com/1145637/2017-world-internet-conference-tim-cook-and-sundar-pichais-surprise-remarks/> [accessed 25 July 2018].

Huaxia. 'President Xi stresses int'l cooperation in cyberspace governance'. *Xinhua.* <http://www.xinhuanet.com/english/2016-11/16/c_135834559.htm> [accessed 20 November 2017].

Hurwitz, Roger. 'The State of Play: Norms and Security in Cyberspace'. *American Foreign Policy Interests.* Vol. 36. No.5. (2014).

Information Office of the State Council of the People's Republic of China. 'The Internet in China'. *Xinhua*. 2010. <http://www.chinadaily.com.cn/china/2010-06/08/content_9950198_7.htm> [accessed 5 May 2018].

Inkster, Nigel. *China's Cyber Power.* Adelphi Series. Vol. 55. No. 456. (2015).

International Telecommunication Union. *Global Cybersecurity Index 2017* <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf> [accessed 20 November 2017].

Interpol. *Cybercrime.* <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> [accessed 25 September 2018].

ITU. *Overview of Cybersecurity. Recommendation ITU-T X.1205.* 2009. <http://www.itu.int/rec/T-REC-X.1205-200804-I/en> [accessed 2 February 2018].

Klimburg, Alexander. *National Cyber Security Framework Manual*. NATO CCD COE. 2012.

Kshetri, Nir. 'Cybercrime and cyber-security issues associated with China: some economic and institutional considerations'. *Electronic Commerce Research.* no. 13. (2013). pp. 41–69.

Lam, Lana & Chen, Stephen. 'US spies on Chinese mobile phone companies, steals SMS data: Edward Snowden'. *South China Morning Post.* 2013. <https://www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden> [accessed 27 November 2017].

Lee, JA, 'The Sino-US Digital Relationship and International *Cyber* Security', in Lemieux F. (eds). *Current and Emerging Trends in Cyber Operations*. Palgrave Macmillan's Studies in *Cyber*crime and *Cyber*security. (Palgrave Macmillan: London. 2015).

Lewis, James Andrew. '4th Meeting of the CSIS-CICIR Cybersecurity Dialogue'. *the Center for Strategic and International Studies (CSIS).* 2011. <https://www.csis.org/events/4th-meeting-csis-cicir-cybersecurity-dialogue> [accessed 19 September 2018].

Li, Cheng. “China’s Communist Party-State: The Structure and Dynamics of Power,” in William A. Joseph, (eds.). *Politics in China An Introduction* (New York: Oxford University Press. 2014).

Lindsay, Jon R. ‘Introduction’, in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, (eds.). *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, (Oxford University Press. 2015).

Markoffaug, John. ‘Before the Gunfire, Cyberattacks’. *New York Times*. 2008. <https://www.nytimes.com/2008/08/13/technology/13cyber.html> [accessed 25 July 2018].

Ministry of Foreign Affairs of the People's Republic of China. *China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel*. 2014 <http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1157487.shtml> [accessed 30 July 2018].

Ministry of Foreign Affairs of the People’s Republic of China. *Full Text: Outcome list of President Xi Jinping’s state visit to the United States*. 2015. <https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1300771.shtml> [accessed 30 June 2018].

Ministry of Foreign Affairs of the People's Republic of China. *Guo Shengkun to Travel to the United States to Co-Chair the First Round of China-US* Law Enforcement and Cyber Security Dialogue. 2017. <https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/wsrc_665395/t1499253.shtml> [accessed 6 October 2018].

Ministry of Foreign Affairs of the People’s Republic of China. *International Strategy of Cooperation on Cyberspace*. 2017. <https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml > [accessed 5 July 2018].

Ministry of Foreign Affairs of the People’s Republic of China. *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference.* 2015. <http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml > [accessed 6 July 2018].

Ministry of Foreign Affairs of the People’s Republic of China. *Study and Implement General Secretary Xi Jinping's Thought on Diplomacy in a Deep-going Way and Keep Writing New Chapters of Major-Country Diplomacy with Distinctive Chinese Features.* 2017. <https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1478497.shtml> [accessed 4 November 2018].

Ministry of Foreign Affairs of the People's Republic of China. *Yang Jiechi's Remarks on the Results of the Presidential Meeting between Xi Jinping and Obama at the Annenberg Estate*. 2013. <https://www.fmprc.gov.cn/mfa_eng/topics_665678/xjpttcrmux_665688/t1049263.shtml> [accessed 28 July 2018].

Mureșan, Radu Constantin. 'Current Approaches Of Diplomacy In The Cyberspace'. (STUDIA UBB. EUROPAEA. Vol. LXII. No. 2. 2017). pp. 31-43.

NATO Cooperative Cyber Defence Centre of Excellence. *Cyber Security Strategy Documents*. <https://ccdcoe.org/cyber-security-strategy-documents.html> [accessed 7 April 2018].

Office of the Press Secretary. *Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting.* 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china- > [accessed 29 June 2018].

Office of the Spokesperson. *U.S.-China Strategic & Economic Dialogue Outcomes of the Strategic Track.* 2016. <https://2009-2017.state.gov/r/pa/prs/ps/2016/06/258146.htm> [accessed 29 June 2018].

Ott, Chris. 'What You Should Know About The 24/7 Cybercrime Network'. Davis Wright Tremaine LLP. 2018. <https://www.dwt.com/files/uploads/documents/publications/What%20You%20Should%20Know%20About%20The%2024.pdf> [accessed 27 September 2018].

Pierini, Gabriele. 'Cyber Security Meets Diplomacy: The EU-NATO Cooperation And The Italian Case. (International University for Social Studies "Guido Carli". 2017).

Potter, Evan H., *Cyber-diplomacy: Managing foreign policy in the twenty-first century*. (Montreal: McGill-Queen's University Press. 2002).

Qingchuan,Yang. 'Commentary: China-U.S. dialogue to transcend talks of cyber security'. *China Central Television.* 2013. <http://english.cntv.cn/20130710/103009.shtml> [accessed 30 June 2018].

Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference. <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint> [accessed 2 December 2017].

Renard, Thomas. *U S-China cybersecurity agreement: a good case of cyber diplomacy*. (2015). http://www.egmontinstitute.be/us-china-cybersecurity-agreement-a-good-case-of-cyber-diplomacy/> [28 December 2017].

Russian Federation. *Order of the Russian Government on signing the agreement between the government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of ensuring international information security*. 2015. <https://*cyber*-peace.org/wp-content/uploads/2013/05/RUSCHN_*Cyber*SecurityAgreement201504_Inofficial Translation.pdf> [accessed 10 August 2018].

Schia, Niels Nagelhus and Gjesvik, Lars. *China's cyber sovereignty*. The Norwegian Institute of International Affairs (2017).

Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era (Delivered at the 19th National Congress of the Communist Party of China October 18, 2017). <http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf> [accessed 24 July 2018].

Segal, Adam. 'Chinese Cyber Diplomacy in a New Era of Uncertainty'. *Hoover Working Group on National security, Technology, and Law*. Aegis Paper Series No. 1703. (Stanford University. 2017).

Segal, Adam. *An Update on U.S.-China Cybersecurity Relations.* 2017. <https://www.cfr.org/blog/update-us-china-cybersecurity-relations> [accessed 23 September 2018].

Segal, Adam. *The Continued Importance of the U.S.-China Cyber Dialogue*. 2017. <https://www.cfr.org/blog/continued-importance-us-china-cyber-dialogue> [accessed 23 September 2018].

Segal, Adam. *U.S. and China in Cyberspace: Uneasy Next Steps*. 2012. <https://www.cfr.org/blog/us-and-china-cyberspace-uneasy-next-steps> [accessed 19 September 2018].

Shanghai Cooperation Organization. *The Shanghai Cooperation Organisation*. 2017. <http://eng.sectsco.org/about_sco/> [accessed 30 February 2018].

Shen, Yi. 'Cyber Sovereignty and the Governance of Global Cyberspace'. *Chinese Political Science Review.* Vol.1. Issue 1. (2016). pp. 81–93.

South China Morning Post. *China seeks to ease Sino-US cyber tensions with top-level talks ahead of Xi Jinping's US trip*. 2015. <https://www.scmp.com/news/china/diplomacy-defence/article/1857903/china-seeks-ease-sino-us-cyber-tensions-top-level-talks> [accessed 4 October 2018].

Sukmadinata, *Metode Penelitian Pendidikan*. (Bandung:Rosdakarya. 2006).

Swaine, Michael D. 'Chinese Views of Cybersecurity in Foreign Relations.' *China Leadership Monitor.* No. 42. (2013).

The Center for Strategic and International Studies (CSIS). *9th Meeting of the CSIS-CICIR Cybersecurity Dialogue*. n.d.. <https://www.csis.org/events/9th-meeting-csis-cicir-cybersecurity-dialogue[accessed 3 October 2018].

The Cyberspace Administration of China. *China-US High-level Joint Dialogue Hotline for Combating Cybercrime and Related Matters.* 2016. <http://www.cac.gov.cn/2016-08/28/c_1119466923.htm> [accessed 25 September 2018].

The Cyberspace Administration of China. *The first meeting of the Central Network Security and Informatization Leading Group held an important speech by Xi Jinping.*

2014. <http://www.cac.gov.cn/2014-02/27/c_133148354.htm> [accessed 16 October 2018].

The Diplomat. *A delegation of Chinese officials visited the U.S. for talks on cybersecurity issues.* 2015. <https://thediplomat.com/2015/09/us-china-hold-cyber-talks-before-xis-visit/> [accessed 30 june 2018].

The State Council Information Office of the People's Republic of China. *China's Military Strategy.* (2015). < http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm> [accessed 20 July 2018].

The State Council Information Office of the People's Republic of China. *International Strategy of Cooperation on Cyberspace.* 2017. <www.scio.gov.cn/32618/Document/1543874/1543874.htm> [accessed 8 April 2018].

The State Council of People's Republic of China. *China, US to jointly fight cyber crime.* 2016. <http://english.gov.cn/state_council/state_councilors/2016/06/15/content_281475372216337.htm> [accessed 4 October 2018].

The White House. *International Strategy for Cyberspace–Prosperity, Security and Openness in a Networked World.* 2011. <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> [accessed 26 November 2017].

Tiirmaa-Klaar, Heli. 'Cyber diplomacy: Agenda, challenges and mission', in K. Ziolkowski (Ed.). *Peacetime regime for state activities in cyberspace: International law, international relations and diplomacy* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 2013).

Tsirigotis, Anthimos Alexandros. *Cybernetics, Warfare and Discourse: The Cybernetisation of Warfare in Britain.* (Springer, 2017).

The State Council The People's Republic of China. *China, US urge maintenance of bilateral dialogue mechanism to combat cybercrime.* 2016. <http://english.gov.cn/state_council/state_councilors/2016/12/08/content_281475510995959.htm> [accessed 3 July 2018].

United Nations, A/70/172. 'Developments in the Field of Information and Telecommunications in the Context of International Security, July 22, 2015' <http://undocs.org/A/70/172> [accessed 5 July 2018].

United Nations, General Assembly, Group of Governmental Experts, A/68/98. 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, June 24, 2013' < http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=/english/&Lang=E > [accessed 5 July 2018].

United Nations Department of Economic and Social Affairs. *Population And Vital Statistics Report Statistical Papers Series A Vol. LXX*. 2018. <https://unstats.un.org/unsd/demographic-social/products/vitstats/sets/Series_A_2018.pdf> [accessed 2 September 2018].

U.S. Department of Justice. *First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes*. 2015. <https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialoguecybercrime-and-related-issues-summary-outcomes-0> [accessed 3 July 2018].

U.S. Department of Justice. *Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue*. 2016. <https://www.justice.gov/opa/pr/second-us-china-cybercrime-andrelated-issues-high-level-joint-dialogue> [accessed 24 September 2018].

U.S. Department of Justice. *Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues*. 2016. <https://www.justice.gov/opa/pr/third-us-china-highlevel-joint-dialogue-cybercrime-and-related-issues> [accessed 24 September 2018].

U.S. Department of State. *Remarks With Chinese Foreign Minister Wang Yi*. 2016. <https://2009-2017.state.gov/secretary/remarks/2016/02/253164.htm> [accessed 5 October 2018].

U.S. Department of the Treasury. *U.S. Fact Sheet – Economic Track Fifth Meeting of the U.S.-China Strategic and Economic Dialogue*. 2013. <https://www.treasury.gov/press-center/press-releases/Pages/jl2011.aspx> [accessed 24 September 2018].

Weihua, Chen. 'China, US to do more on cyber crime'. *China Daily*. 2016. <http://usa.chinadaily.com.cn/a/201612/08/WS5a30d69da3108bc8c672f523.html> [accessed 5 October 2018].

Xinhua. 'Commentary: Pentagon's annual China military report exposes U.S. Cold War mentality'. *People's Daily*. 2012. <http://en.people.cn/102774/7821676.html> [accessed 9 September 2018].

Xinhua. 'Attacks originating from U.S. rank first among overseas hackings in China: FM.'. *Global Times*. 2013. <http://www.globaltimes.cn/content/762961.shtml > [accessed 17 July 2018].

Xinhua. *China's digital economy accounts for 30% of 2016 GDP: Report*. 2017. <http://www.chinadaily.com.cn/business/4thwic/2017-12/05/content_35212111.htm> [accessed 24 November 2017].

Xinhua. *China is victim of cyber attacks: spokesman*. 2012. <http://www.chinadaily.com.cn/china///2012-03/29/content_14946469.htm> [accessed 14 July 2018].

Xinhua. *Online crime continues to rise in China*. 2017. <http://www.chinadaily.com.cn/china/2017-10/16/content_33329294.htm> [accessed 9 February 2018].

Xinhua. *Procuratorates approve arrest of 19,000 telecom fraud suspects*. 2017. <http://news.xinhuanet.com/english/2017-01/14/c_135982423.htm> [accessed 29 July 2018].

Xinhuanet. *The First Meeting of the Central Cyber Security and Informationization Leading Group Held an Important Speech by Xi Jinping*. 2014. <http://www.cac.gov.cn/2014-02/27/c_133148354.htm> [accessed 24 July 2018].

Zhang, Jian. 'China's new foreign policy under Xi Jinping: towards 'Peaceful Rise 2.0'?'. *Global Change, Peace & Security*. 27:1. (2015). pp. 5-19.

Zheng, Ye. 'From Cyberwarfare to Cybersecurity in the Asia-Pacific and Beyond', in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, (eds.). *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. (Oxford University Press. 2015).

Ziolkowski, Katharina. 'Confidence Building Measures for Cyberspace', in K. Ziolkowski (Ed.), *Peacetime regime for state activities in cyberspace: International law, international relations and diplomacy* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. 2013).